BINARY ADDERS TO IMPROVE ENERGY EFFICIENT USING QUANTUM DOT CELLULAR AUTOMATA

Kannan.D [1], Subash.M [2], V.B.Bhapith [3]

[1,2] U.G Student, Department of Electronics and Communication Engineering,
Raja College of Engineering and Technology, Madurai, Tamilnadu,(India)
[3] Assistant Professor, Department of Electronics and Communication Engineering,
Raja College of Engineering and Technology, Madurai, Tamilnadu, (India)

ABSTRACT

As transistors decrease in size more and more of them can be accommodated in a single die, thus increasing chip computational capabilities. However, transistors cannot get much smaller than their current size. The quantum-dot cellular automata (QCA) approach represents one of the possible solutions in overcoming this physical limit, even though the design of logic modules in QCA is not always straightforward. Many logical circuits are designed using QCA which consume low power. Designing of adders using QCA. Increase on number of new results on adders. To design adders and detailed simulation using QCAD designer. The performance is increased by adder. Delay performance compared to Ripple carry adder (RCA).

Keywords: QCA CELL, RCA Adder

I. INTRODUCTION

Quantum Dot cellular Automata (QCA) don't use transistors. Basic element of QCA is a quantum cell; each quantum cell has electrons in them. Electron transmission occurs on the columbic interaction of the electrons. QCA encodes binary information in the charge configuration within a cell. QCA is an advanced research program and efforts are made to reduce the complexity of the circuits. In this brief, an innovative technique is presented to implement high-speed low-area adders in QCA. Theoretical formulations demonstrated for CLA and parallel-prefix adders are here exploited for the realization of a novel 2-bit addition slice. The latter allows the carry to be propagated through two subsequent bit-positions with the delay of just one majority gate (MG). In addition, the clever top level architecture leads to very compact layouts, thus avoiding unnecessary clock phases due to long interconnections.

II. QCA CELL

A quantum-dot cellular automata (QCA) is a square nanostructure of electron wells having free electrons. Each cell has four quantum dots. The four dots are located in the four corners. The cell can be charged with two free electrons.

Logic 0 logic 1

A QCA is a nanostructure having as its basic cell a square four quantum dots structure charged with two free electrons able to tunnel through the dots within the cell. Because of Columbic repulsion, the two electrons will always reside in opposite corners. The locations of the electrons in the cell (also named polarizations P) determine two possible stable states that can be associated to the binary states 1 and 0.

Even though these addition circuits use different topologies of the generic FA, they have a carry-in to carry-out path consisting of one MG, and a carry-in to sum bit path containing two MGs plus one inverter. As a consequence, the worst case computational paths of the n-bit RCA and the n-bit CFA consist of (n+2) MGs and one inverter.

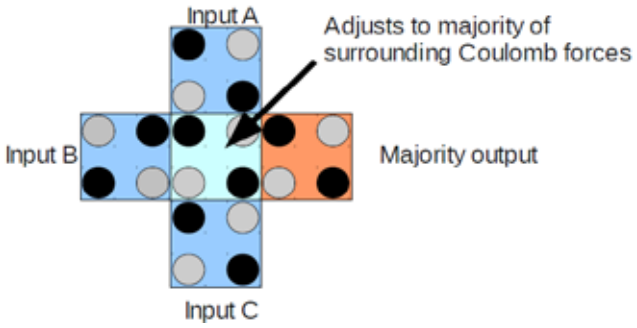


Figure 1: QCA Majority Voter

In particular, the auxiliary propagate and generate signals, namely pi = ai + bi and gi = ai · bi , are computed for each bit of the operands and then they re grouped four by four. Such a designed n-bit CLA has a computational path composed of 7+4×(log4 n) cascaded MGs and one inverter. This can be easily verified by observing that, given the propagate and generate signals (for which only one MG is required), to compute grouped propagate and grouped generate signals; four cascaded MGs are introduced in the computational path. In addition, to compute the carry signals, one level of the CLA logic is required for each factor of four in the operands word-length. This means that, to process nbit addends, log4 n levels of CLA logic are required, each contributing to the computational path with four cascaded MGs. When n-bit operands are processed, its worst case computational path consists of 4×log2 n−3 cascaded MGs and one inverter. Apart from the level required to compute propagate and generate signals, the prefix tree consists of 2 × log2n − 2 stages.

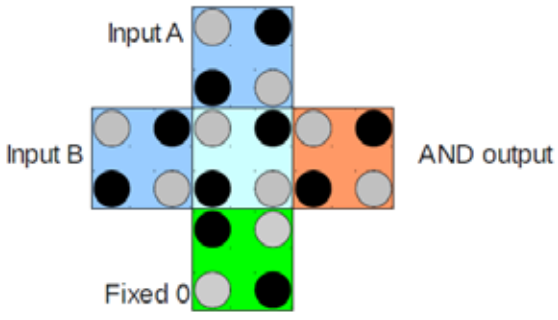


Figure 2: And Gate

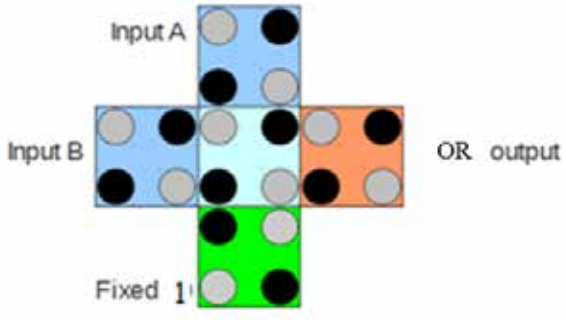


Figure 3: Or Gate

To introduce the novel architecture proposed for implementing ripple adders in QCA, let consider two n-bit addends A = an−1. . . a0 and B = bn−1. . . b0 and suppose that for the i th bit position (with i = n − 1. . . 0) the auxiliary propagate and generate signals, namely pi = ai + bi and gi = ai · bi , are computed. ci being the carry produced at the generic (i−1)th bit position, the carry signal ci+2, furnished at the (i+1)th bit position, can be

computed using the conventional CLA logic reported. In this way, the RCA action, needed to propagate the carry ci through the two subsequent bit positions, requires only one MG.

Conversely, conventional circuits operating in the RCA fashion, namely the RCA and the CFA, require two cascaded MGs to perform the same operation. In other words, an RCA adder designed as proposed has a worst case path almost halved with respect to the conventional RCA and CFA.

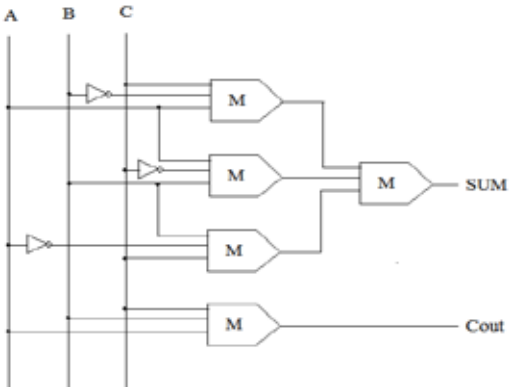


Figure 4: Conventional Adder

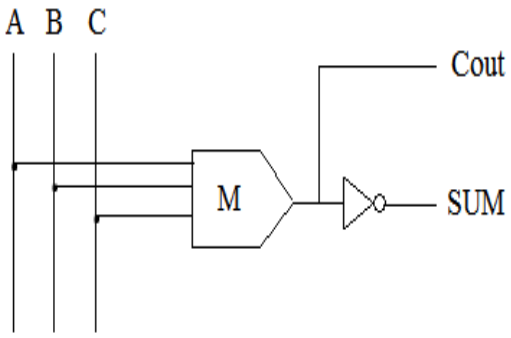


Figure 5: Conventional Adder

III. RESULTS AND DISCUSSION

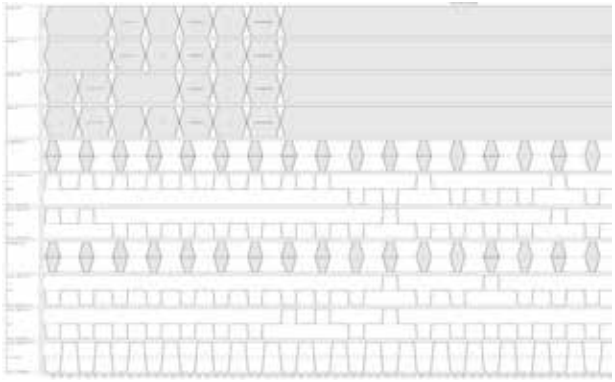


Figure 5: Adder with 64 bit

IV. CONCLUSION

A new adder designed in QCA was presented. It achieved speed performances higher than all the existing QCA adders, with an area requirement comparable with the cheap RCA and CFA demonstrated. The novel adder operated in the RCA fashion, but it could propagate a carry signal through a number of cascaded MGs significantly lower than conventional RCA adders. In addition, because of the adopted basic logic and layout strategy, the number of clock cycles required for completing the elaboration was limited. A 64-bit binary adder designed as described in this brief exhibited a delay of only nine clock cycles, occupied an active area of 19.72 μm2, and achieved an ADP of only 169.48.

REFERENCES

[1] C. S. Lent, P. D. Tougaw, W. Porod, and G. H. Bernestein, “Quantum cellular automata,” Nanotechnology, vol. 4, no. 1, pp. 49–57, 1993.

[2] M. T. Niemer and P. M. Kogge, “Problems in designing with QCAs: Layout = Timing,” Int. J. Circuit Theory Appl., vol. 29, no. 1, pp. 49–62, 2001.

[3] J. Huang and F. Lombardi, Design and Test of Digital Circuits by Quantum-Dot Cellular Automata. Norwood, MA, USA: Artech House, 2007..

[4] W. Liu, L. Lu, M. O'Neill, and E. E. Swartzlander, Jr., "Design rules for quantum-dot cellular automata," in Proc. IEEE Int. Symp. Circuits Syst., May 2011, pp. 2361–2364.

[5] K. Kim, K. Wu, and R. Karri, "Toward designing robust QCA architectures in the presence of sneak noise paths," in Proc. IEEE Design, Autom. Test Eur. Conf. Exhibit., Mar. 2005, pp. 1214–1219.

PARALLEL FILTER USING ERROR CORRECTION CODES IN MODERN SIGNAL PROCESSING CIRCUITS

Sulthan Alavudeen.S [1], Samuvel Paul Raj [2], Ajith Kumar [3]

[1,2,3] U.G Student, Department of Electronics and Communication Engineering,
Raja College of Engineering and Technology, Madurai, Tamilnadu, (India)

ABSTRACT

Digital filters are widely used in signal processing and communication systems. In some cases, the reliability of those systems is critical, and fault tolerant filter implementations are needed. Next many techniques that exploit the filters' structure and properties to achieve fault tolerance have been proposed. As technology scales, it enables more complex systems that incorporate many filters. In those complex systems, it is common that some of the filters operate in parallel, for example, by applying the same filter to different input signals. Recently, a simple technique that exploits the presence of parallel filters to achieve fault tolerance has been presented. In this brief, that idea is generalized to show that parallel filters can be protected using error correction codes (ECCs) in which each filter is the equivalent of a bit in a traditional ECC. This new scheme allows more efficient protection when the number of parallel filters is large. The proposed scheme coded in HDL and simulated using xilinx 12.1 e.

Keywords: Error correction codes (ECCs), filters, and soft errors.

I. INTRODUCTION

Electronic circuits are increasingly present in automotive, medical, and space applications where reliability is critical. In those applications, the circuits have to provide some degree of fault tolerance. This need is further increased by the intrinsic reliability challenges of advanced CMOS technologies that include, e.g., manufacturing variations and soft errors. A number of techniques can be used to protect a circuit from errors. Those range from modifications in the manufacturing process of the circuits to reduce the number of errors to adding redundancy at the logic or system level to ensure that errors do not affect the system functionality.

$$y[n] = \sum_{l=0}^{\infty} x[n-l] \cdot h[l]$$

Where x[n] is the input signal, y[n] is the output, and h[l] is the impulse response of the filter.

When the response h[l] is nonzero, only for a finite number of samples, the filter is known as a FIR filter, otherwise the filter is an infinite impulse response (IIR) filter impulse response of the filter

II.PROPOSED SYSTEM

The new technique is based on the use of the ECCs. A simple ECC takes a block of *k* bits and produces a block of *n* bits by adding *n−k* parity check bits . The parity check bits are XOR combinations of the *k* data bits. By properly designing those combinations it is possible to detect and correct errors. As an example, let us consider

a simple Hamming code [14] with $k = 4$ and $n = 7$. In this case, the three parity check bits $p1$, $p2$, $p3$ are computed as a function of the data bits $d1$, $d2$, $d3$, $d4$ as follows:

$$p1 = d1 \oplus d2 \oplus d3$$
$$p2 = d1 \oplus d2 \oplus d4$$
$$p3 = d1 \oplus d3 \oplus d4.$$

- Based on the use of the ECCs
- Error Correction Codes (ECCs) using each of the filter outputs
- It can correct failures in multiples modules
- *In The Parity, the error is detected and corrected by using,*
  - $yc1[n] = z1[n] - y2[n] - y3[n]$

The data and parity check bits are stored and can be recovered later even if there is an error in one of the bits. This is done by recomputing the parity check bits and comparing the results with the values stored. In the example considered, an error on $d1$ will cause errors on the three parity checks; an error on $d2$ only in $p1$ and $p2$; an error on $d3$ in $p1$ and $p3$; and finally an error on $d4$ in $p2$ and $p3$. Therefore, the data bit in error can be located and the error can be corrected.

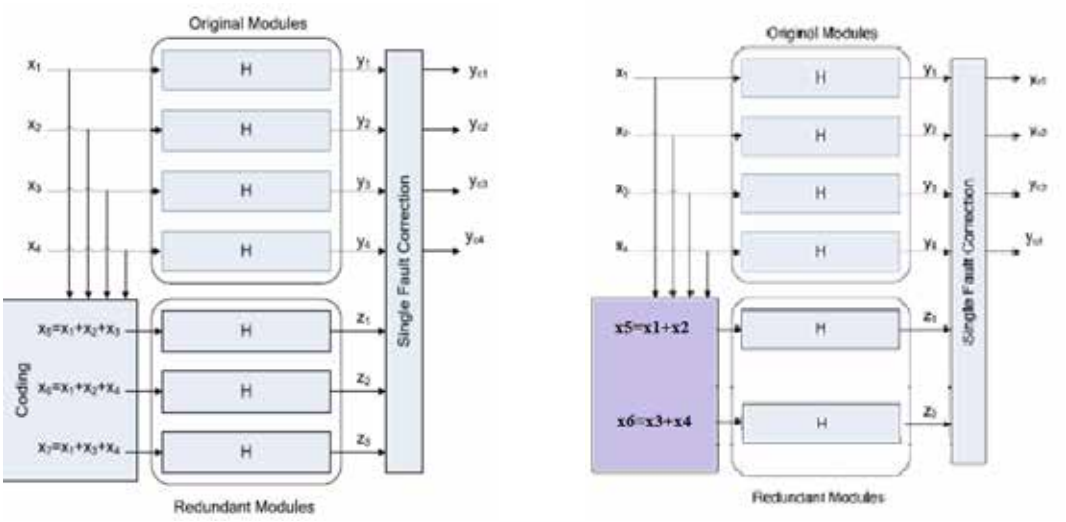


Figure 1: Block Diagram of Proposed Work

This ECC scheme can be applied to the parallel filters considered by defining a set of check filters $z\,j$. For the case of four filters $y1$, $y2$, $y3$, $y4$ and the Hamming code, the check filters would be

$$z1[n] = y1[n] + y2[n] + y3[n]$$
$$z2[n] = y1[n] + y2[n] + y4[n]$$
$$z3[n] = y1[n] + y3[n] + y4[n]$$

For example, an error on filter $y1$ will cause errors on the checks of $z1$, $z2$, and $z3$. Similarly, errors on the other filters will cause errors on a different group of zi . Therefore, as with the traditional ECCs, the error can be located and corrected.

III. RESULTS AND DISCUSSION

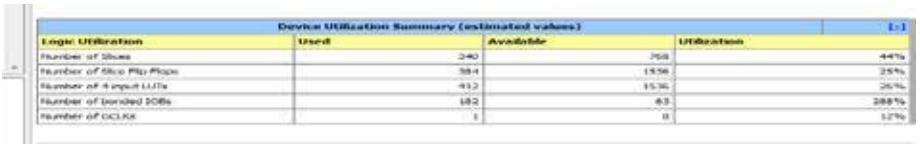


Figure 2: Design Summary

S.NO	PARAMETER	EXISTING METHOD	PROPOSED
1	NUMBER OF SLICES	428	340
2	IOB'S	208	182
3	LUT'S	558	412

Figure 3: Performance Analysis of Proposed Work

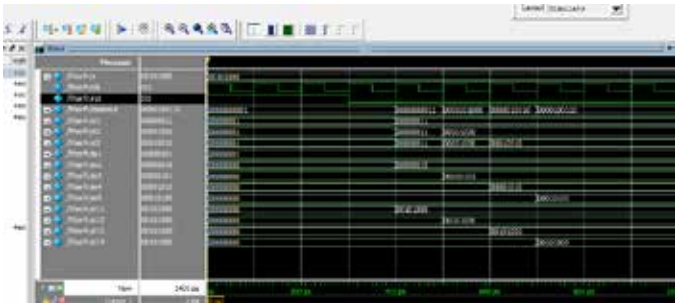


Figure 4: Simulation of Proposed Work

IV. CONCLUSION

In this project, we have presented a scheme to protect parallel filters that are commonly found in modern signal processing circuits. The approach is based on applying ECCs to the parallel filters outputs to detect and correct errors. The proposed scheme can also be applied to the FIR filters The technique is evaluated using a only two redundant filter to achieve the high error correction in ECC which also reduces the area, delay and power than previous. This will be of interest when the number of parallel filters is small as the cost of the proposed scheme is larger in that case.

REFERENCES

[1] B. Shim and N. Shanbhag, "Energy-efficient soft error-tolerant digital signal processing," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 14, no. 4, pp. 336–348, Apr. 2006.

[2] T. Hitana and A. K. Deb, "Bridging concurrent and non-concurrent error detection in FIR filters," in *Proc. Norchip Conf., 2004, pp. 75–78.*

[3] Y.-H. Huang, "High-efficiency soft-error-tolerant digital signal processing using fine-grain subword-detection processing," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 18, no. 2, pp. 291–304, Feb. 2010.*

[4] S. Pontarelli, G. C. Cardarilli, M. Re, and A. Salsano, "Totally fault tolerant RNS based FIR filters," in *Proc. IEEE IOLTS, Jul. 2008*, pp. 192–194.

[5] Z. Gao, W. Yang, X. Chen, M. Zhao, and J. Wang, "Fault missing rate analysis of the arithmetic residue codes based fault-tolerant FIR filter design," in *Proc. IEEE IOLTS, Jun. 2012, pp. 130–133.*

ATTENDANCE SYSTEM USING NFC TECHNOLOGY AND EMBEDDED CAMERA DEVICE ON MOBILE PHONE

R.RajaMurugan [1], T.Rohan [2], G.SakthiSankaraPandian [3]

[1,2,3] U.G Student, Department of Electronics and Communication Engineering,
Raja College of Engineering and Technology, Madurai, Tamilnadu, (India)

ABSTRACT

This project proposes the design and development to create a system that makes easier to check students' attendance automatically, and this system is implemented in based on NFC technology. Registering for attendance in education environments especially universities is a highly demanding activity as a result of increasing number of students. The attendance process normally involves circulating a paper for the students to register their names, or the lecturer calling the names and registering the students either in a paper or from PDA/PC. In the first case the students' attention may be attracted while taking the lectures and at the same time they can register for students who do not being present in the class.

Keywords: NFC technology, NFC mobile application smart attendance system, wireless attendance system

I. INTRODUCTION

In the most of Thailand universities, instructors take attendance by calling out the names and surnames of students, and then marking them, while, in others, instructors pass around a sheet of paper, asking students to sign in attendance sheet just next to their surnames. Both practices have their drawbacks. In the first case, if numerous groups attend the lesson, checking all of these students by name and surname might take about several minutes out of each lesson; in the second case, friends of absent students may write down their names and surnames. These practices place university instructors and their institutions at considerable disadvantages when it comes to taking attendance. To rectify these systematic failings, we have desire to put the NFC tag into service. Each tag has a unique ID, precluding the duplication of a tag. These NFC tag are given to students of Apply Mathematic department, Faculty of and while students entering classrooms and touch these tag on instructor mobile phone, NFC readers program on instructor's mobile phone will read these tags, identify the students from their respective NFC tag and send the data to an instructor's mobile phone. Mobile phone, in turn, sends all the data it has collected to the server by the end of lesson, or at the end of this day according to the preference of lecturer. This means no class time will be wasted.

II. EXISTING SYSTEM

Currently Some universities prefer to use paper sheet for controlling attendance, whereas some universities prefer to use paper sheet for checking students' attendance and after this, fill out these information into a system manually.

III. PROPOSED SYSTEM

This paper propose to create a system with one server PC to which all NFC device are connected, so all data will be saved in one database on server PC and send to the database on the server too, making the monitoring of the information effortless. All instructors must have a NFC device with an embedded NFC reader that can read student NFC tag, as well as an embedded camera device on mobile phone that can take their photos. The camera device is meant to prevent a student from giving his/her NFC tag to a classmate who attends the lecture, touch the other student's NFC tag to make it appear as if s/he had also attended. When a student enters class and touch his/her NFC tag on instructor's mobile phone, the NFC reader reads his/her student NFC tag, while the camera device on mobile phone simultaneously takes his/her photo and sends it to the database in instructor's mobile phone.

After some time, the instructor submits all data for backup in a database server. When students enter the classroom and touch theirs NFC tag near instructor's NFC device the NFC reader on mobile phone automatically reads their NFC tag and the embedded camera device on takes their photos as NFC or near-field communication, is an easy and intuitive technology that allows user to use user's mobile phone for special purposes. An NFC tag can share and link to information such as web pages, social media and all other sorts of other information generally. Other areas where NFC is starting to evolve into are making payments, opening doors secured with contactless locks, logging on to computers and many more. All of these actions have something in common, that is they invoke an action based on user placing NFC device near (the N in NFC) the thing user want to read or interact with. NFC is bridging the gap between both the physical and virtual worlds. By bringing two devices near each other, there is a virtual reaction. Bluetooth and Wi-Fi do not have this ease in set up. So the key feature of NFC is automatic and there is no need to launch an MATLAB application.

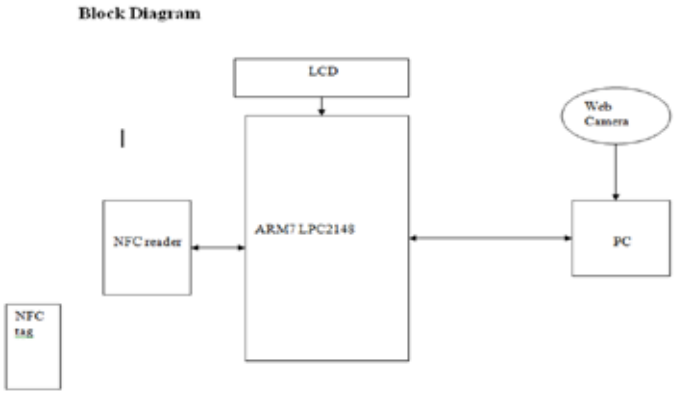


Figure 1: Block Diagram of Proposed Work

3.1 ARM 7

The LPC2141/2/4/6/8 microcontrollers are based on a 32/16 bit ARM7TDMI-S CPU with real-time emulation and embedded trace support, that combines the microcontroller with embedded high speed flash memory ranging from 32 kB to 512 kB. A 128-bit wide memory interface and unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces code by more than 30 % with minimal performance penalty. Due to their tiny size and low power consumption, LPC2141/2/4/6/8 are ideal for applications where miniaturization is a key requirement, such as access control and point-of-sale. A blend of serial communications interfaces ranging from a USB 2.0 Full Speed device, multiple UARTS, SPI, SSP to I2Cs and on-chip SRAM of 8 kB up to 40 kB, make these devices very well suited for communication gateways and protocol converters, soft modems, voice recognition and low

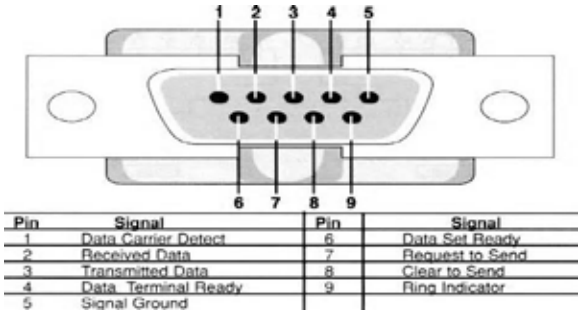
end imaging, providing both large buffer size and high processing power. Various 32-bit timers, single or dual 10-bit ADC(s), 10-bit DAC,

PWM channels and 45 fast GPIO lines with up to nine edge or level sensitive external interrupt pins make these microcontrollers particularly suitable for industrial control and medical systems. 16/32-bit ARM7TDMI-S microcontroller in a tiny LQFP64 package.

- 8 to 40 kB of on-chip static RAM and 32 to 512 kB of on-chip flash program memory. 128 bit wide interface/accelerator enables high speed 60 MHz operation.
- In-System/In-Application Programming (ISP/IAP) via on-chip boot-loader software.
- Single flash sector or full chip erase in 400 ms and programming of 256 bytes in 1 ms.
- EmbeddedICE RT and Embedded Trace interfaces offer real-time debugging with the on-chip RealMonitor software and high speed tracing of instruction execution.
- USB 2.0 Full Speed compliant Device Controller with 2 kB of endpoint RAM.
- In addition, the LPC2146/8 provide 8 kB of on-chip RAM accessible to USB by DMA.
- One or two (LPC2141/2 vs. LPC2144/6/8) 10-bit A/D converters provide a total of 6/14 analog inputs, with conversion times as low as 2.44 µs per channel.
- Single 10-bit D/A converter provides variable analog output.
- Two 32-bit timers/external event counters (with four capture and four compare channels each), PWM unit (six outputs) and watchdog.
- Low power real-time clock with independent power and dedicated 32 kHz clock input.
- Multiple serial interfaces including two UARTs (16C550), two Fast I2C-bus (400 kbit/s), SPI and SSP with buffering and variable data length capabilities.
- Vectored interrupt controller with configurable priorities and vector addresses.
- Up to 45 of 5 V tolerant fast general purpose I/O pins in a tiny LQFP64 package.
- Up to nine edge or level sensitive external interrupt pins available. 60 MHz maximum CPU clock available from programmable on-chip PLL with settling time of 100 µs.
- On-chip integrated oscillator operates with an external crystal in range from 1 MHz to 30 MHz and with an external oscillator up to 50 MHz.
- Power saving modes include Idle and Power-down.
- Individual enable/disable of peripheral functions as well as peripheral clock scaling for additional power optimization.
- Processor wake-up from Power-down mode via external interrupt, USB, Brown-Out
- Detect (BOD) or Real-Time Clock (RTC).
- Single power supply chip with Power-On Reset (POR) and BOD circuits:
  - CPU operating voltage range of 3.0 V to 3.6 V (3.3 V ± 10 %) with 5 V tolerant I/O

Figure 2: ARM Processor

An RS-232 serial port was once a standard feature of a personal computer, used for connections to modems, printers, mice, data storage, uninterruptible power supplies, and other peripheral devices. However, RS-232 is hampered by low transmission speed, large voltage swing, and large standard connectors. In modern personal computers, USB has displaced RS-232 from most of its peripheral interface roles. Many computers do not come equipped with RS-232 ports and must use either an external USB-to-RS-232 converter or an internal expansion card with one or more serial ports to connect to RS-232 peripherals. RS-232 devices are widely used, especially in industrial machines, networking equipment and scientific instruments.



Pin	Signal	Pin	Signal
1	Data Carrier Detect	6	Data Set Ready
2	Received Data	7	Request to Send
3	Transmitted Data	8	Clear to Send
4	Data Terminal Ready	9	Ring Indicator
5	Signal Ground		

Figure 3: Serial Port

IV. CONCLUSION

The system presented in this project will substantially improve the current day's attendance registration system and eliminate many paper works involved in it. Other benefits include eliminating the chance of losing attendance data, different attendance reports can be easily generated by a click of mouse, simplifying the decision making process related to attendance, etc. One of the major distinct characteristics of our proposed system is that the hardware required is minimal, i.e. Only NFC tag and NFC-enabled mobile device.

REFERENCES

[1] V. Coskun, K. Ok, and B. Ozdenizci, Near Field Communication: From Theory to Practice, 1st ed., West Sussex, United Kingdom: John Wiley & Sons, 2011.

[2] M. A. Ayu, T. Mantoro, S. A. Ismail, and N. S.Zulkifli, “Rich Information Service Delivery to Mobile Users Using Smart Posters,” presented at the 2nd International Conference on Digital Information and Communication Technology (DICTAP) 2012, Bangkok, Thailand,16-18 May 2012, ISBN: 978-1-4673-0734-5.

[3] S. K. Jain, U. Joshi, and B. K. Sharma, “Attendance Management System,” Masters Project Report, Rajasthan Technical University, Kota.

[4] M. Mattam, S. R. M. Karumuri, and S. R. Meda, “Architecture for Automated Student Attendance,” in Proc. IEEE Fourth International Conference on Technology for Education (T4E 2012), pp.164-167,18-20 July 2012, doi: 10.1109/T4E.2012.39.

[5] Z.-G. Zhang, P. Gong, L.-J. Cao, and Y.-L. Chen, “Information Technologies and Applications in Education,” First IEEE International Symposium on Digital Object Identifier, 2007, pp.606–609.

[6] M. K. P. Basheer and C. V. Raghu, “Fingerprint attendance system for classroom needs,” in Proc. India Conference (INDICON), 2012 Annual IEEE, pp. 433-438, 7-9 Dec. 2012.

IMAGE DENOISING TO ESTIMATE THE GRADIENT HISTOGRAM PRESERVATION USING VARIOUS ALGORITHMS

P.Mahalakshmi[1], J.Muthulakshmi[2], S.Kannadhasan[3]

[1,2] U.G Student, [3] Assistant Professor, Department of Electronics and Communication Engineering, Raja College of Engineering and Technology, Madurai, Tamilnadu, India.

ABSTRACT

Natural image statistics plays an important role in image denoising and various natural image priors, including gradient-based have been widely studied and exploited for noise removal. Image denoising aims to estimate the latent clean image from its noisy observation .We apply the pre-processing method using histogram equalization. In our project we propose a textures enhanced image denoising method by enforcing the gradient histogram of the denoised image to be close to a reference gradient histogram of the original image and to enhance the texture structures while removing noise.

Keywords: Denoising, GHP, B-GHP, S-GHP, Histogram

I.INTRODUCTION

Image denoising is a classical yet still active topic in image processing and low level vision, while it is an ideal test bed to evaluate various statistical image modeling methods. With the rapid development of digital imaging technology, now the acquired images can contain tens of megapixels. On one hand, more fine scale texture features of the scene will be captured; on the other hand, the captured high definition image is more prone to noise because the smaller size of each pixel makes the exposure less sufficient. Unfortunately, suppressing noise and preserving textures are difficult to achieve simultaneously, and this has been one of the most challenging problems in natural image denoising. Unlike large scale edges, the fine scale textures are much more complex and are hard to characterize by using a sparse model. Texture regions in an image are homogeneous and are composed of similar local patterns, which can be characterized by using local descriptors. Using histogram specification, a gradient histogram preservation algorithm is developed to ensure that the gradient histogram of denoised image is close to the

Reference histogram, resulting in a simple yet effective GHP based denoising algorithm.

II. RELATED WORK

Generally, image denoising methods can be grouped in two categories: model-based methods and learning-based methods. The use of gradient prior can be traced back to 1990s when Rudin et al. They proposed a total variation (TV) model for image denoising , where the gradients are actually modeled as Laplacian distribution. Another well-known prior model, the mixture of Gaussians, can also be used to approximate the distribution of image gradient. More generally, the local sparsity prior can be well applied to high-pass filter responses, wavelet transform coefficients, or the coding coefficients over a redundant dictionary. In Gaussian scale mixtures are

used to characterize the marginal and joint distributions of wavelet transform coefficients. However, many existing image denoising algorithms, including those local sparsity and NSS based ones, tend to wipe out the image fine scale textures while removing noise. Popular prior is the nonlocal self-similarity (NSS) prior; the natural images are often many similar patches (i.e., nonlocal neighbors) to a given patch, which may be spatially far from it. Sparse representation for image leads to State of the art image denoising results; often fail to preserve the image fine scale texture structure. Large scale edges, the fine scale textures are more complex and are hard to characterize by using sparse model.

III. PROPOSED METHOD

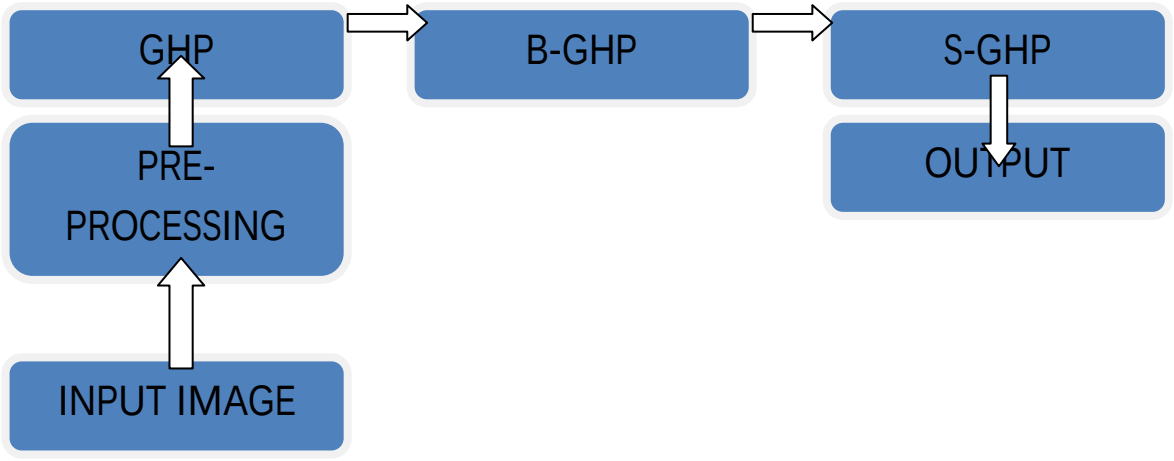


Figure 1: Block Diagram of Proposed Work

We introduce the gradient histogram estimation and preservation framework. It presents the denoising model and the iterative histogram specification algorithm (IHSA). It also introduces two region-based GHP variants, i.e., B-GHP and S-GHP. By segmenting the image into texture homogeneous regions, S-GHP can further achieve better denoising results than B-GHP in terms of PSNR.

3.1 Pre-Processing

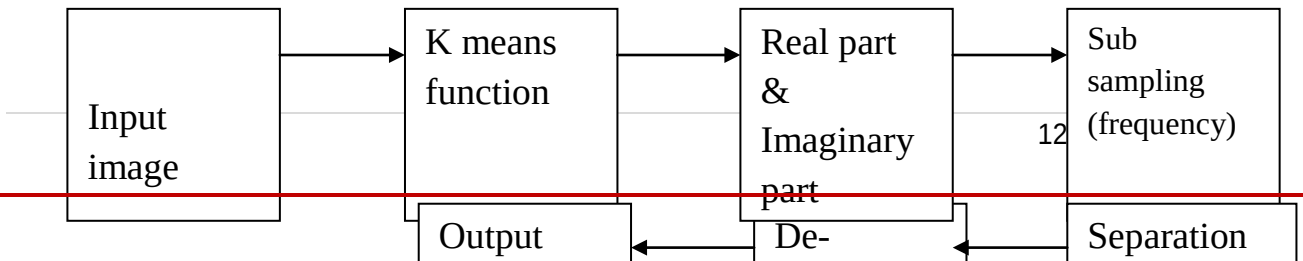
In our project, we are implementing histogram equalization for our input image. A histogram is a graphical representation of the distribution of data. The data appears as colored or shaded rectangles of variable area.

3.2 Histogram Equalization

Histogram equalization uses a non-linear and monotonic mapping. The idea of histogram equalization is that the pixels should be distributed evenly over the whole intensity range. The aim is to transform the image so that the output images has a flat histogram.

3.3 Gradient Histogram Preservation (Ghp):

We propose a texture enhanced image denoising method by enforcing the gradient histogram of original image. Different combinations of pixel brightness values (gray levels) occur in a pixel pair in an image. An GHP algorithm is also developed to effectively estimate the gradient histogram from the noisy observation of the image.



By simply partitioning the image into regular blocks, the block based B-GHP can reduce the possibility of generating false textures.

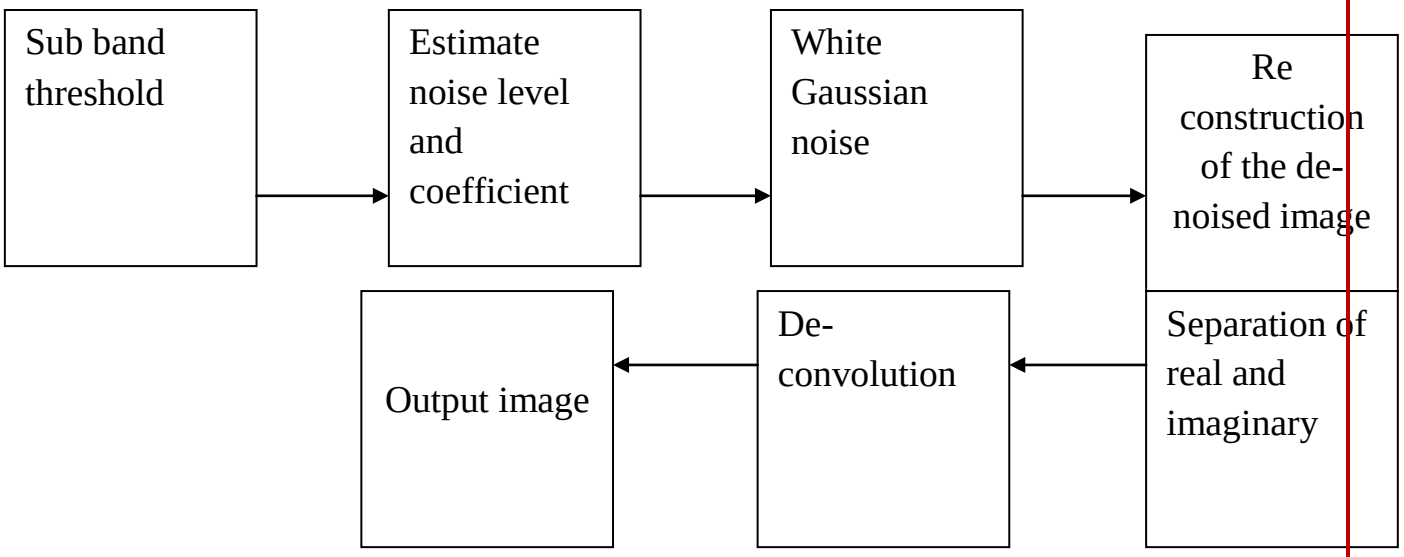


Figure 3: Block Diagram of S-GHP

We then compare S-GHP with some state-of-the-art denoising methods, including shape-adaptive by segmenting the regions. In contrast, S-GHP preserves much better the fine textures in areas of tree and water, making the denoised image looks more natural and visually pleasant. It should also be noted that, the better visual quality in areas of tree and water of S-GHP might not always result in higher PSNR. S-GHP preserves much better the fine texture in tree and water areas, while making the output look more natural. One strategy is to transform the noisy image into an image with additive white Gaussian noise (AWGN) and then apply GHP. Finally it is avoided in our proposed system.

IV. RESULTS AND DISCUSSION

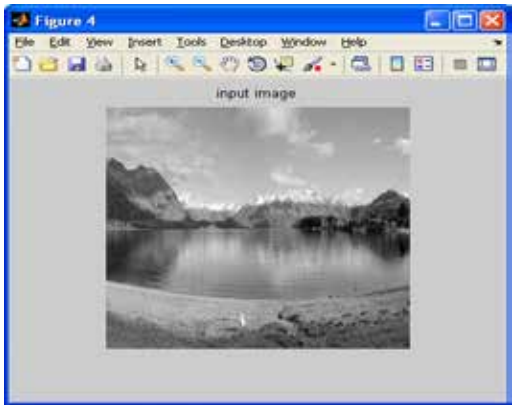


Figure 4 : Input Image

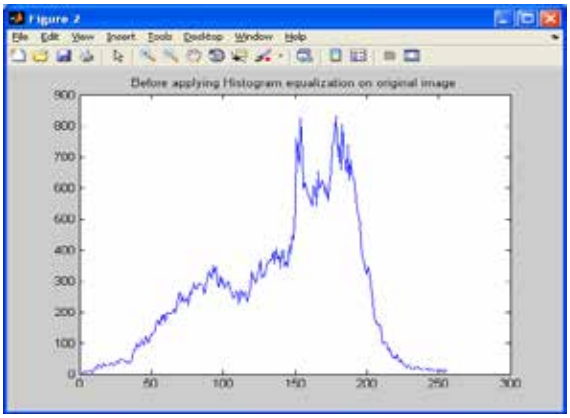
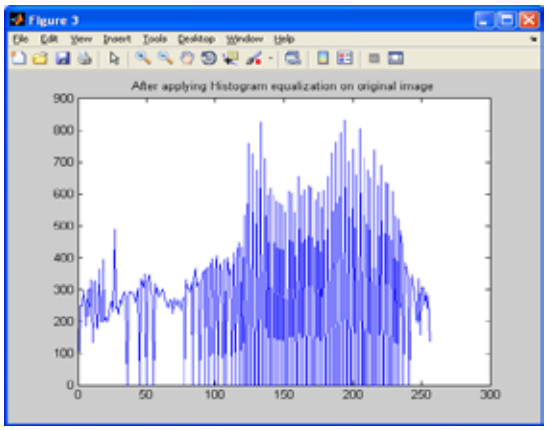


Figure 4: Before applying Histogram equalization



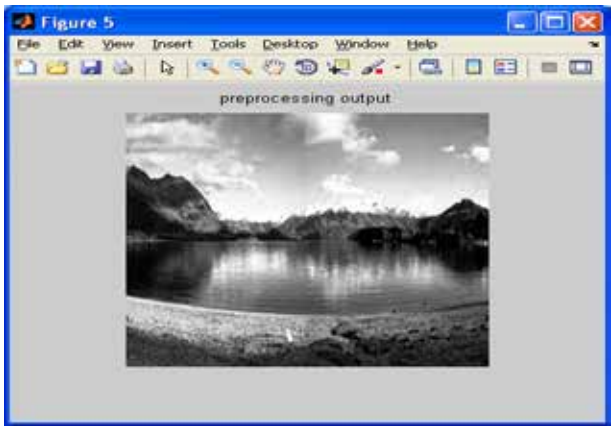
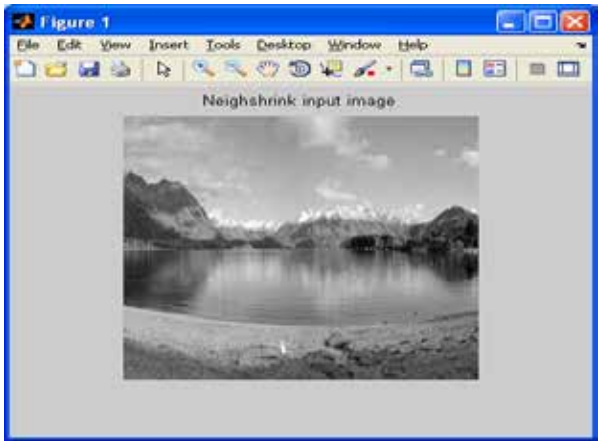
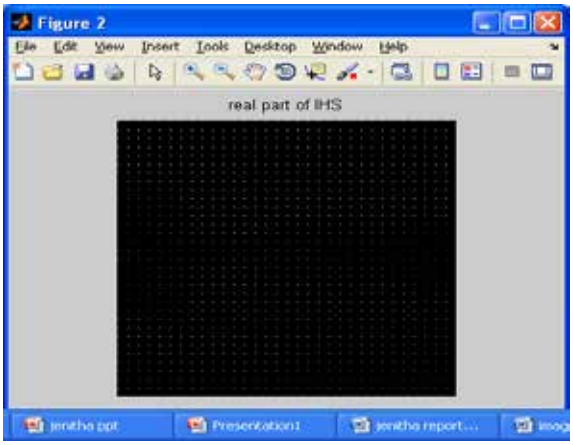


Figure 5: After applying Histogram equalization **Figure 6: Pre-processing output**





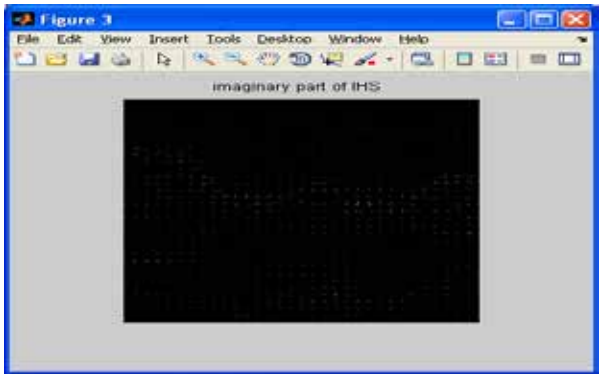


Figure 7: Real and Imaginary Part of HIS **Figure 8: HIS Interpolation**

Output Parameters in GHP

PSNR =31.8478

MSE = 42.4909

V. CONCLUSION

In our project we propose a textures enhanced image de-noising method by enforcing the gradient histogram of the de-noised image to be close to a reference gradient histogram of the original image and to enhance the texture structures while removing noise. B-GHP and S-GHP, which leads to improve SNR values compared to GHP. S-GHP can further achieve better de-noising results than B-GHP in terms of PSNR. Less mean square error compared to GHP and B-GHP.

REFERENCES

[1] R. Fergus, B. Singh, A. Hertzmann, S. Roweis, and W. T. Freeman, "Removing camera shake from a single photograph," in Proc. ACM SIGGRAPH, 2006, pp. 787–794.

[2] A. Levin, R. Fergus, F. Durand, and W. T. Freeman, "Image and depth from a conventional camera with a coded aperture," in Proc. ACM SIGGRAPH, 2007.

[3] D. Krishnan and R. Fergus, "Fast image deconvolution using hyper- Laplacian priors," in Proc. NIPS, 2009, pp. 1033–1041.

[4] L. Rudin, S. Osher, and E. Fatemi, "Nonlinear total variation based noise removal algorithms," Phys. D, vol. 60, nos. 1–4, pp. 259–268, Nov. 1992.

[5] M. Wainwright and S. Simoncelli, "Scale mixtures of Gaussians and the statistics of natural images," in Proc. NIPS, vol. 12. 1999, pp. 855–861.

[6] J. Portilla, V. Strela, M. J. Wainwright, and E. P. Simoncelli, "Image denoising using a scale mixture of Gaussians in the wavelet domain," IEEE Trans. Image Process, vol. 12, no. 11, pp. 1338–1351, Nov. 2003.

[7] M. Elad and M. Aharon, "Image denoising via sparse and redundant representations over learned dictionaries," IEEE Trans. Image Process, vol. 15, no. 12, pp. 3736–3745, Dec. 2006.

[8] W. Dong, L. Zhang, G. Shi, and X. Wu, "Image deblurring and super resolution by adaptive sparse domain selection and adaptive regularization," IEEE Trans. Image Process, vol. 20, no. 7, pp. 1838–1857, Jul. 2011.

[9] A. Buades, B. Coll, and J. Morel, "A review of image denoising methods, with a new one," Multiscale Model. Simul., vol. 4, no. 2, pp. 490–530, 2005.

AN ETHNOBOTANICAL STUDY OF MEDICINAL PLANTS USED IN SACRED GROVES OF AMBAJI FOREST, GUJARAT, INDIA.

Dr. R. S. Patel

Associate Professor, KKSJ Maninagar Science College, Ahmedabad, Gujarat,(India.)

ABSTRACT

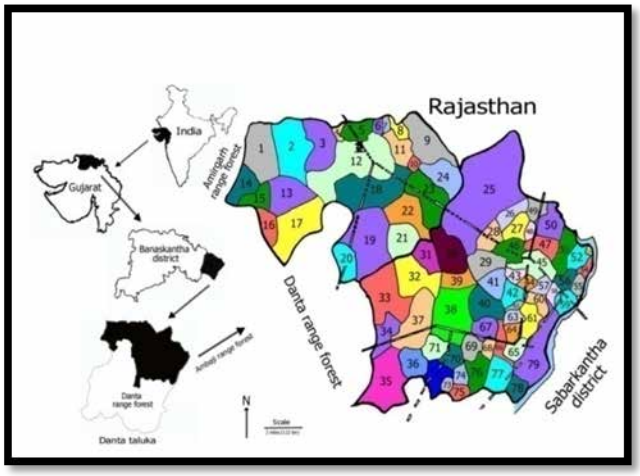
Gujarat is situated in the Central Western part of India, with an area of 1, 96,020 Sq. km. Ambaji range forest belonging to Banaskantha District. It is a part of Ambaji-Balaram wildlife sanctuary. Ambaji range forest is a part of Danta taluka of 300 sq. km. geographical area of the range. North Gujarat is following under Boswellia forest type[1]. The adivasi (local people) dwelling in the forest have good knowledge of herbal medicine. The term 'Ethnobotany' was first coined[2] encompasses entire studies concerning plants, which describe local people interaction with the natural environment. Its scope was much elaborated later. Present Ethnobotany links diverse disciplines such as anthropology, botany, linguistics, nutrition, ecology, conservation, economics and pharmacology, opening a wide field yet to enrich the human knowledge[3] Present paper deals with an ethnobotanical study of medicinal plants used in sacred groves like Babo Dev SGS: (Village-Meen), Khandor mata SGS (Village-Sebaliya), Mamaji SGS (Village -Chikhla), and Rakhevad Bavji SGS (Village-Halad) of ambaji forest are enumerated. The 31 plant species belonging to 25 families are gathered and explained its exact botanical name with family, local name and folk uses for number of diseases. These sacred groves are being protected for generations together to maintain the unique diversity, endemic, medicinal and useful valued species. Extensive field trips were carried out in the sacred grove at monthly intervals. Specimens of flowering plants were collected and identified with the aid of different regional floras.

Key Words: Medicinal Plants, Sacred Groves, Ambaji forest.

I. INTRODUCTION

Banaskantha, Sabarkantha, Mehsana and Patan are the four districts of North Gujarat, among them in Banaskantha district the Danta and Ambaji range forests are the part of Danta taluka having the part of Aravalli hills. Ambaji range forest is a part of Danta taluka situated on eastern part of the Banaskantha district in North Gujarat. Ambaji range forest is a part of Danta taluka situated on eastern part of the Banaskantha district in North Gujarat. These forests are inhabited by a variety of ethnic groups including the tribes like Bubadiya, Parghi, Taral, Bhemiyat, Dhrangi, Khair, Laur, Makwana, Dabhi, Solanki, Chauhan, Gamar, Parmar, Rohisa, Rathod, Mansi, Damor, Khermal, Kodarvi etc. These tribes cover 48 per cent of the total population. Out of 300 sq. km. geographical area of the range, about 542 sq. km is notified as Ambaji-Balaram wildlife sanctuary. The two main rivers Banas and Sabarmati and their tributaries are contributing to the enrichment of floral components. The average annual rainfall is about 725mm. Ambaji range forest is representing 434 angiosperm species (20% of the Gujarat flora) belonging to 85 families. The forest type is dry deciduous and scrub

(Champion and Seth, 1968) harbors about 400 tracheophyte plant species, including pteridophytes, gymnosperms and angiosperms. These forest areas are inhabited by around 20 tribes. The present investigation was carried out in Ambaji range forest of Banaskantha district of North Gujarat. Tribal people of Ambaji forest range directly depend upon forest resources for their daily needs. Tribal people of Ambaji forest range directly depend upon forest resources for their daily needs. The aim of Ethnobotany is to study how and why people use and conceptualize plants in their local environments. Plants have been used in the traditional healthcare from time immemorial, particularly among tribal communities[4]. Total 37 Plants species belonging to 26 families documenting of sacred groves and sacred plants of Jhalod and surrounding areas, Gujarat[5]. Sacred groves are one of the way to of the conservation of biodiversity. while trying to understand and document the indigenous knowledge of resource management practices. Collection and Removal of Any Material from the Sacred Groves is prohibited[6-7]. Sacred groves or sacred trees serve as a home for birds and mammals, and hence, they indirectly help in the conservation of living organisms[8] The Sacred groves found in different regions of India posses rich diversity of medicinal plants and provide suitable habitat for their sustainable, natural regeneration[9-11]. Protection of a large number of medicinal plants in sacred forests of different parts of India is some of the well documented by earlier studies[12-14]. It is also observed that more than 35,000 plant species are being used around the world for medicinal purposes[15]. The communities residing in these rich biodiversity areas have rich traditional wisdom of herbal medicines. Almost every village has a Bhuva (tantric/cosmic healers), a Bhagat (religios healers) or a Vaida (herbal healers) who are carriers of the traditional Knowledge. This is much evident from various studies and documentation undertaken in the past in the areas of ethno-botany, ethno-medicine\, tribal culture, livelihood, veterinary medicine etc[16-20].



Study Area Map

II. MATERIALS AND METHODS

The study area was surveyed regularly to record the floristic wealth of sacred grove of Ambaji forest areas. Various field trips were arranged and specimens were collected, identified with the help of Flora of the Presidency of Bombay[21] and Gujarat Flora[22] and properly processed through standard methods. Special note on the ethno botany were noted. Plant species were arranged according to Bentham and Hooker's classification given in the Gujarat Flora. Here documented 31 plant species were belonging to 29 genera and 25 families. Field notes with special reference to their distributional and regeneration status were noted. Followings are of

some important contributors worked on North Gujarat flora: Plants of North Gujarat and Floristic study of North Gujarat[23-25]

Data Collection From various Tribal People of Ambaji Forest, Gujarat during Different extensive fieldtrips (2012-2014)

Fig: A Babo Dev SG (Village Meen) Fig: B Khandor mata SG (Village Seba

Fig: C Mamaji SG (Village Chikhla) Fig: D Rakhevad Bavji SG (Village Halad)

Fig: E Preparation of Herbarium of Medicinal plants in KKSJ Lab. Ahmedabad, Gujarat

III. RESULTS AND DISCUSSION

Critical Observations from Study area:

The information about ethno botanical plants from the various Sacred groves and Sacred plants were collected from the tribal of this area. Fig: A to Fig:D Shows different groves at Ambaji forest Fig: E Shows Herbarium preparation in KKSJ Research lab., Ahmedabad, Plate 1 Shows Informators of different Sacred groves Table 1 Checklist of Sacred plants reported from certain Sacred groves. Table 2 Shows Dicot and Monocot ratio of the various ethno medicinal plants, Fig 1 Shows Dicot and Monocot ratio of the various Sacred plants, Table:3 Synoptic view of different plant species reported from the study areas Fig:2 Synoptic view of different plant species reported from the study areas

The Following are the Medicinal plants frequently found and used by the tribals of Ambaji forest.

1. ***Miliusa tomentosa* (Roxb.) Sinclair** [UMPH, UMBIYO]; Annonaceae
   - Fresh roots are tied at abdomen to cure tumors [Jivabhai].
2. ***Crateva nurvala* Buch.-Ham.** [VAYVARNO]; Capparaceae
   - Dried bark paste is applied twice a day on abscess [Somabhai].
3. ***Flacourtia indica* (Burm. f.) Merr.** [KANTI]; Flacourtiaceae
   - Few root pieces are boiled in water and applied on the poisonous animal bites [Somabhai].
4. ***Bombax ceiba* L.** [SIMLO, SAVAR]; Bombacaceae
   - About 100g of fresh inner bark is crushed into paste and applied on broken horn of cattle. It sets well in few days. [Nopabhai].
   - Fresh stem bark paste (paste is made by rubbing stem bark on a moist stone) and applied on skin diseases and pimples. [Somabhai].
5. ***Grewia hirsuta* Vahl.** [SISOTI[; Tiliaceae
   - A glassfull of stem extract is taken in the morning with empty stomach to join bones of human beings and cattles [Khemabhai].
6. ***Aegle marmelos* (L.) Coee.** [BILI]; Rutaceae
   - Boiled fresh leaves are applied for blood clotting [Arjanbhai].
   - Ripe fruits are edible and having medicinal properties [Shirmiben].
7. ***Boswellia serrata* Roxb.** [SALAD, DHUPELIO, GUGAL]; Burseraceae
   - Fresh leaves paste discrled water and bathing with this cures vomiting [Somabhai].
8. ***Azadirachta indica* A. Juss.** [NEEM, LIMDO]; Meliaceae
   - Inner bark is mixed with blackpepper, salt and water. The mixture is taken thrice a day to cure fever. [Arjanbhai].
9. ***Sapindus laurifolius* Vahl.** [ARITHU]; Sapindaceae
   - Boiled leaf juice is given to children for curing vomiting. Leaves are used as fodder [Devabhai].
   - About 50ml of fresh leaf juice is taken regularly to cure fever after delivery [Somabhai].

10. ***Mangifera indica* L.** [KERI, AMBO]; Anacardiaceae
    - Dried malformed inflorecence are powdered and given with water to animals, as a cure for swollen stomach [Somabhai].
11. ***Butea monosperma* (Lam.) Taub.** [KHAKHRO, KESUDO]; Papilionceae
    - About 250g fresh stem-bark is crushed with water and filterate is taken once in a day to cure diarrhoea [Somabhai].
12. ***Delonix elata* (L.) Gamble** [HINDRO, SANDSRO]; Caesalpiniaceae
    - Four to five leaves are crushed with water and paste is made it is applied on eyelids for removal of eye diseases [Somabhai].
13. ***Acacia nilotica* (L.) Del. subsp. *indica* (Bth.) Brenan** [BAVAL]; Mimosaceae
    - 100ml of stem bark decoction is taken once a day to cure stomach pain [Anabhai].
    - Leaf juice is given to cure sunstroke [Jivabhai].
14. ***Anogeissus latifolia* (Roxb.) Wall. ex Bedd.** [DHAVDO]; Combretaceae
    - Fifty grams of fresh stem bark is chewed regularly for curing cough [Jibvabhai].
15. ***Terminalia bellirica* (Gaern.) Roxb.** [BEHDR, BEHDA]; Combretaceae
    - About 5g of fruit powder is mixed with a glass of water and taken twice a day to cure sleeplessness. [Jivabhai].
16. ***Alangium salvifolium* (L. f.) Wang.** [ANKOLI, ANKOL]; Alangiaceae
    - About 100g fresh roots are rubbed with water and applied on the poisionous animal sting [Jivabhai].
17. ***Adina cordifolia (Roxb.)* Bth. & Hk. f. ex Brandis** [HALDU]; Rubiaceae
    - About 200g fresh stem bark is boiled in 400ml water, with sugar or honey. The mixture taken twice in a day to cure jaundice [Devabhai].
    - Five inch piece of fresh stem bark is crushed with water and applied on mumps [somabhai].
18. ***Diospyros melanoxylon* Roxb.** [TIBRU, TIMBRU]; Ebenaceae
    - Dried stem bark is smok is inhaled to cure Asthma [Somabhai].
19. ***Holarrhena antidysenterica* (L.) Wall ex G. Don** [KUDA, DOLA KUDA]; Apocynaceae
    - Fresh roots are crushed with water, a tea spoonfull of this filterate is taken once a day early in the mornnig cures diarrhoea [Nopabhai].
    - About 25g fresh roots are pounded with 100ml water and taken one spoonful as a for cure stomach pain [Nanabhai].
20. ***Cordia dichotoma* Forsk.** [VADGUNDO, MOTOGUNDO]; Boraginaceae
    - A glass of fresh leaf juice is taken thrice a day regularly to women as pain killer after delivery [Jivabhai].
21. ***Cordia gharaf* (Forsk.) F. N. Will** [GUNDI, NANI GUNDI]; Boraginaceae
    - A tea spoonfull of stem bark juice is given orally to cure dysentry [Somabhai].
    - About 50ml of leaf juice is given to cure dysentry.[Jivalabhai].
22. ***Tecomella undulata* (Sm.) Seem** [RAGAT ROHIDO]; Bignoniaceae
    - A teaspoonful of leaf juice is taken thrice a day to cure fever [Somabhai].

- A tea spoonful of flowers powder is taken thrice a day regularly to cure cancer [Karimbhai].

23. ***Clerodendrum multiflorum* (Burm. f) O . Ktze.** [ARNI]; Verbenaceae
    - About 100 gms fresh leaves or soft stem branches are crushed and poultice is made used to relieve eye pain [Jivabhai].
24. ***Lantana camara* L.** [DHANI DHARIYA]; Verbenaceae
    - Leaf paste is applied on animal ulcers [Devabhai].
25. ***Vitex negundo* L.** [NAGOD]; Verbenacaeae.
    - Leaf paste is applied on rheumatic swellings [Devabhai and Somabhai].
26. ***Euphorbia nerifolia* L.** [THOR]; Euphorbiaceae
    - Fresh leaf paste is applied on abscess [Arjanbhai].
27. ***Jatropha curcas* L.** [RATANJOT]; Euphorbiaceae
    - Lalex is applied to cure toothache [Jallobhai].
28. ***Ficus benghalensis* L.** [VAD, VALLO]; Moraceae
    - Yellow old leaves are steamed and applied on abdomen to cure stomach pain [Devabhai].
29. ***Ficus racemosa* L.** [UMARO]; Moraceae
    - Fresh latex is applied on tongue to cure cough [Somabhai].
30. ***Phoenix sylvestris* (L.) Roxb.** [KHAJURI]; Arecaceae
    - A teaspoonful of root juice is taken twice a day to cure stomach pain [Nopabhai].
31. ***Dendrocalamus strictus* Nees.** [LAKADI]; Poaceae
    - Young shoot paste is applied externally to stop bleeding [Somabhai].

Plate 1 Informators of the study area

Table 1 Checklist of Medicinal plants frequently reported from certain Sacred groves.

Sr no.	Botanical name	Local name	Family
1.	*Miliusa tomentosa* (Roxb.) Sinclair	UMPH, UMBIYO	Annonaceae
2.	*Crateva nurvala* Buch.-Ham.	VAYVARNO	Capparaceae
3.	*Flacourtia indica* (Burm. f.) Merr.	KANTI	Flacourtiaceae
4.	*Bombax ceiba* L.	SIMLO, SAVAR	Bombacaceae
5.	*Grewia hirsuta* Vahl.	SISOTI	Tiliaceae
6.	*Aegle marmelos* (L.) Coee.	BILI	Rutaceae
7.	*Boswellia serrata* Roxb.	SALAD, DHUPELIO, GUGAL	Burseraceae
8.	*Azadirachta indica* A. Juss.	NEEM, LIMDO	Meliaceae
9.	*Sapindus laurifolius* Vahl.	ARITHU	Sapindaceae
10.	*Mangifera indica* L.	KERI, AMBO	Anacardiaceae
11.	*Butea monosperma* (Lam.) Taub.	KHAKHRO, KESUDO	Fabaceae
12.	*Delonix elata* (L.) Gamble	HINDRO, SANDSRO	Caesalpiniaceae
13.	*Acacia nilotica* (L.) Del. subsp. indica (Bth.) Brenan	BAVAL	Mimosaceae
14.	*Anogeissus latifolia* (Roxb.) Wall. ex Bedd.	DHAVDO	Combretaceae
15.	*Terminalia bellirica* (Gaern.) Roxb.	BEHDR, BEHDA	Combretaceae
16.	*Alangium salvifolium* (L. f.) Wang.	ANKOLI, ANKOL	Alangiaceae
17.	*Adina cordifolia* (Roxb.) Bth. & Hk. f. ex Brandis	HALDU	Rubiaceae
18.	*Diospyros melanoxylon* Roxb.	TIBRU, TIMBRU	Ebenaceae
19.	*Holarrhena antidysenterica* (L.) Wall ex G. Don	KUDA, DOLA KUDA	Apocynaceae
20.	*Cordia dichotoma* Forsk.	VADGUNDO, MOTOGUNDO	Boraginaceae
21.	*Cordia gharaf* (Forsk.) F. N. Will	GUNDI, NANI GUNDI	Boraginaceae
22.	*Tecomella undulata* (Sm.) Seem	RAGAT ROHIDO	Bignoniaceae
23.	*Clerodendrum multiflorum* (Burm. f) O . Ktze.	ARNI	Verbenaceae
24.	*Lantana camara* L.	DHANI DHARIYA	Verbenaceae
25.	*Vitex negundo* L.	NAGOD	Verbenacaeae.

26.	*Euphorbia nerifolia* L.	THOR	Euphorbiaceae
27.	*Jatropha curcas* L.	RATANJOT]	Euphorbiaceae
28.	*Ficus benghalensis* L.	VAD, VALLO	Moraceae
29.	*Ficus racemosa* L.	UMARO	Moraceae
30.	*Phoenix sylvestris* (L.) Roxb.	KHAJURI	Arecaceae
31.	*Dendrocalamus strictus* Nees.	LAKADI	Poaceae

Table 2 Dicot and Monocot ratio of the various ethno medicinal Plants

Dicot	**29**
Monocot	**02**

Fig 1 Dicot and Monocot ratio of the various ethno medicinal Plants

Table:3 Synoptic view of different plant species reported from the Study area

Species	**31**
Genus	**29**
Family	**25**

Fig:2 Synoptic view of different plant species reported from the Study area

IV. SUMMARY AND CONCLUSION

The range forest is having a series of Aravalli hills with dry deciduous scrub forests. *Butea monosperma, Holarrhena antidysenterica, Wrightia tinctoria, Lannea coromandelica, Boswellia serrata, Zizyphus mauritiana* etc are found mostly in hilly regions. Species like *Soymida febrifuga, Morinda tomentosa, Ougeinia oojeinensis, Hymenodictyon excelsum, Schrebera swietenioides, Oroxylum indicum, Tecomella undulata, Bridelia retusa* are found with restricted distribution. Out of these tree species, *Ougeinia oojeinensis* one of the potential medicinal species used for women delivery was found very rare. 4 species of pteridophytes are recorded in shady areas in the forest. Local inhabitants of the present study area are greatly dependent on the forest resources. It was observed that the tribal villagers were collecting fire wood from forest and selling in nearby towns. Habitat destruction due to grazing, logging, agriculture conversion of forest into land and road constructions is causing rapid disappearance of many floral components. Interviews conducted with local inhabitants during the study period showed ethnobotanical use of about 42 plant species by various tribal communities[26]. Some of the informators bio-data along with their photograph are also provided. Survey on ethnobotanical practice of the area showed a good number tree species have been used for the preparation of various agricultural implements, household implements, musical instruments etc. There is considerable decrease in use of plant resources through traditional way. Sometimes limited availability of phytowealth causing erosion of ethnobotanical practices. It is felt that further intensive ethnobotanical explorations are needed to bring out valuable information. Since the present study was mainly based on visual observation, further studies are necessary to document the potential medicinal plants both qualitatively and quantitatively.

V. ACKNOWLEDGEMENT

I am highly indebted to my dearest guide, Dr. A. S. Reddy for his invaluable guidance, painstaking efforts and moral boost constantly provided during the tenure.I am very grateful to the all the local healers, local vendors, local tribal inhabitants and forest officials, Ambaji forest division for their valuable cooperation, also grateful to the UGC (University Grant Commission, Pune) for financial support of this project and Principal, Dr. R. R. Shah for giving me this opportunity. I would like to thanks my students Aayushi Purohit and Smruti Jain for their timely help and enthusiastic support.

REFERENCES

Journal papers

[1] Champion, H.G. and Seth, S.K. (1968). *A revised survey of forest types of India,* Forest Research of India, DEHRADUN, (UTTARAKHAND) India.

[2]. Harshberger, J. W. 1895. Some new ideas: The plants cultivated by aboriginal people and how used in primitive commerce. *The (daily) Evening Telegraph. Philadelphia.* 64 (134) : 2.

[3]. Balick, M. K. and Cox, P. A. 1996. *Plants, People and Culture: The Science of Ethnobotany.* Scientific American Libraray, New York.

[4] Laloo, R. C., Kharlukhi, L., Jeeva, S. and Mishra, B. P. 2006. Status of medicinal plants in the disturbed and the undisturbed sacred forests of Meghalaya, northest India : population structure and regeneration efficacy of some important species. *Current Science,* 90(2) : 225-231.

[5]. Maru R.N. and Patel R.S.(2013) Ethnobotanical Survey of Sacred Groves and Sacred Plants of Jhalod and Surrounding areas in Dahod District,Gujarat,India.Research Journal of Recent Sciences Vol.2(ISC-2012),130-135 (2013) ISSN 2277-2502

[6]. Khan M.L.,Rai J.P.N. and Tripathi R.S., Population Structure of Some Tree Species in Disturbed and protected sub-tropical forests of north-aast India, *Acta Ecologica*, 8(3), 247-255(1987)

[7]. Khiewtam R.S. and Ramakrishnan P.S., Socio-cultural studies of the sacred groves at Cherrapunji and adjoining areas in North Eastern India, Man in India, 69(1),64-71 (1989)

[8]. Islam A.K.M.N., Islam M.A. and Hogue A.E. Species composition of sacred groves, their diversity and conservation in Bangladesh. In: Ramakrishnan, P.S., Saxena, K.G. and Chandrasekhar, U.M(Editors), Conserving the Sacred for Biodiversity Management. UNESCO and Oxford-IBH Publishing, New Delhi Pages, 163-165 (1998).

[9]. Ved D K, Parithima C L, Morton Nancy and Darshan S, Conservations of Indian's medicinal plant diversity through a novel approach of establishing a network of insitu gene banks, In: Uma Shankar R, Ganeshaiah K N and Bawaks (eds) Forest Genetic Resources: Status Threats and Conservation Strategies, (Oxford and IBH New Delhi) (2001).

[10]. Boraiah K.T., Vasudeva R., Shonil A. and Kushalappa C.G., Do informally managed sacred groves have higher richness and regeneration of medicinal plants than state – managed reserve forests?., Curr Sci, 84, 804 (2003).

[11]. Airi S., Rewal R.S., Dhar U. and Purohit A.N., Assessment of availability and habitat preference of JAtamansi – a critically endangered medicinal plant of west Himalaya, Curr Sci, 79, 1467 (2000).

[12] Vartak V.D., Kumbhojkar M S and Nipuge DS, Sacred groves in tribal areas of Western Ghats: treasure trove of medicinal plants, *Bulletin of Medico-Ethno-Botanical Research*, 8, 77-78(1987).

[13]. Bhakat R.K. and Pandit P.K., Role of a sacred grove in conservation of medicinal plants, *Indian Forester, 129, 224-232 (2003)*

[14]. Bhakat R., and pandit P.K., An inventory of medicinal plants of some sacred geoves of purulia District West Bengal, *Indian Forester*, 130, 37-43(2004)

[15]. Sukumaran S., Raj ADS Medicinal Plants Sacred groves in Kanyakumari district, southern Western Ghats, Indian J. Trad, Knowl, 9(2) 294-299(2010).

[16]. Bedi S. J. (1968). Floristic Study of Ratanmahal and Surrounding Hills. A Phd thesis submitted to the M. S. University of Baroda. Vol. I & II.

[17]. Oza, (1991) Taxonomical and Ecological Studies of The Flora of and Around Bhavnagar.

[18]. Punjabi, B. L. (1998) An Ethnobotanical study of Tribal areas of District Sabarkantha(North Gujarat). Ph.D. Thesis submitted to North Gujarat University, Patan.

[19]. Shah, G.L (1983) Rare species with restricted distribution in south Gujarat. In: S.K. Jain & R. R. Rao. (eds) An Assessment of Threatened Plants of India. Bot. Surv. India, Calcutta. P. 50-54.

[20]. Umadevi, A.J. (1988). Identification and status survey of medicinal plants of Gujarat. Ph.D. Thesis South Gujarat University, Surat.

Books:

[21]. Cooke, Theodore. (1958). *Flora of the Presidency of Bombay*. Vol. 1, 2, & 3. Botanical Survey of India, Calcutta (reprint).

[22]. Shah, G. L. (1978).*Flora of Gujarat State*. Vol. I & II. Sardar Patel University Press, Vallabh Vidyanagar.

Thesis:

[23]. Patel, K.C. (2002). Floristics and Ethnobotanical Studies on Danta Forest of North Gujarat; Ph.D Thesis, Sardar Patel University, Vallabh Vidyanagar (GUJARAT) INDIA.

[24]. Saxton, W.T. and L.J. Sedgwick Plants of Northen Gujarat, Rec. Bot, Surv., India, 9, 207-323 (1918).

[25]. Yogi, D. V. (1970).*A contribution to the flora of North Gujarat*; Ph.D. Thesis, S.P. University, Vallabh Vidyanagar.

[26]. Patel, R.S. (2002). Floristics and Ethnobotanical Studies on Ambaji Forest of North Gujarat; Ph.D. Thesis, Sardar Patel University, Vallabh Vidyanagar (GUJARAT) INDIA.

USAGE OF ASSOCIATION RULE MINING IN COURSE SELECTION FOR INDUSTRIAL TRAININGS

Pratiyush Guleria[1], Manu Sood[2]

[1, 2] *Department of Computer Science, Himachal Pradesh University, Shimla, Himachal Pradesh, (India)*

ABSTRACT

This paper focuses on usefulness of Association Rule Mining in Education and Councelling.Knowledge extracted using ARM will be helpful in decision making for students to determine courses chosen for industrial trainings. In this paper, we are deriving preferable courses for pursuing trainings for students based on course combinations. Here, two measures are used for deciding the usefulness of an association rule i.e. support and confidence and only those rules are selected which satisfy both a minimum support and a minimum confidence threshold.

Keywords: ARM, Councelling, Confidence, Decision, Education, Support.

I. INTRODUCTION

In data mining, association rule learning is a method for discovering interesting relations between variables in large databases [1]. ARM task is to discover the hidden association relationship between the different item sets in transaction database [2]. An X⇒Y type association rule expresses a close correlation between items in a database [3]. Association rules provide information in the form of if-then statements and they are probabilistic in nature. If part is the antecedent and then part is the consequent. Association rules analyzes the antecedent and consequent for set of items called item set that are disjoint having no items in common and for examining each row in database, user has to set two threshold values i.e. the first value is called the support for the row and the second is called the confidence for the row."Support" is simply the number of transactions that includes all the items in the antecedents and consequent part of the row. It can sometimes be expressed as percentage of total number of records in the database. In ARM [4], rules are selected only if they satisfy both a minimum support and a minimum confidence threshold.

Support of the rule A=>B is shown in Eq .1

support (A=>B[s, c]) = p(AUB) = support ({A, B}) ---------- (1)

s,c represents support and confidence. Eq. 1 denotes the frequency of the rule within all transactions in the database i.e. the probability that a transaction contains both A and B and Eq. 2 denotes the percentage of transactions containing A which also contains B i.e. the probability that a transaction containing A also contains B [5].

Confidence of the rule A=>B is shown in Eq.2

confidence (A=>B[s, c]) = p (B|A) = p(AUB)/p(A)

= support ({AUB})/support ({A}) ---------- (2)

Table I shows the hypothetical list of course combinations taken by students for their industrial trainings. Here each row is considered as transaction, each comprising a combination of variables or item sets. From Table I, strong rules are derived shown in Table II with Rule Support and Rule Confidence. Threshold values assumed for Support is 0.3 and Confidence is 0.75.

TABLE I. Hypothetical List of Course Combinations

SID	Courses Combination(X)	Preferable Course(Y)
1	Java,J2EE	Android
2	Java,J2EE,HTML	Android
3	HTML,Javascript	PHP
4	C,C++	Asp.Net
5	J2EE,Java	Android
6	C,C++	Java
7	C,C++,VB.Net	Java
8	C,C++	Java
9	HTML	PHP
10	HTML,Asp.net	PHP
11	----------	--------

TABLE II Rule Support and Confidence

Rules	Rule Support	Rule Confidence
Java,J2EE=> Android	0.3	1
HTML=>PHP	0.3	0.75
C,C++=>Java	0.3	0.75

II. LITERATURE REVIEW

In [6], author has discussed about image classification using Association Rule Mining with decision tree algorithm. Association Rule Mining task is to find out hidden relationships between different item sets. Enrique Garcia et.al [3] describes a collaborative educational data mining tool based on association rule mining. This tool helps in improvement of e-learning courses and allows teachers to analyze and discover hidden information based on interaction between the students and the e-learning courses. According to Ruijuan Hu [1], Data Mining based on Association Rules is playing important role in Medical Field. Using Association Rule learning interesting relations between variables in large databases are discovered and Apriori is the best known algorithm to mine association rules. In [4], author has applied ARM approach in social-science related fields such as education and Councelling. Mirela Danubianu, Stefan Gheorghe Pentiuc and Iolanda Tobolcea [7] conducted a case study on mining association rules inside a Relational Database. In [8], author presents association rule mining for Students Assessment Data. Student's performance can be analyzed using Association Rule Mining. In [9], author presents data mining in education environment that identifies student's failure patterns using ARM technique. Author in [10] has done Frequent Pattern Mining with WEKA tool using Apriori Algorithm. Stefan Mutter, Mark Hall, and Eibe Frank [11] have used classification approach to evaluate the output of Confidence-Based Association Rule Mining. In [12], author has worked on a problem of mining association rules between

items in a large database of sales transactions using PHP as front-end and MySQL database and analyzed buying habits of customers for improving sales.

III. MINING USING APRIORI ALGORITHM

Apriori algorithm given by Agrawal & Srikant is the best known algorithm to mine association rules. Apriori Algorithm is having a property which states that all nonempty subsets of a frequent item set must also be frequent and an item set is any subset of all the items in the database. Table III shows the steps followed by Apriori algorithm.

TABLE III. Steps Followed by APRIORI Algorithm

Step 1	Initially make a single pass over the dataset to determine the support of each item.
Step 2	Find all frequent 1-itemsets.
Step 3	Iteratively generate new candidate set for 2-itemset, 3 –item set and so on from the frequent item sets found in the previous iterations.
Step 4	Repeat step 2 for finding all frequent 2-itemsets, 3 item sets.
Step 5	Support for each candidate is then counted and checked against the minsup threshold value given.
Step 6	Algorithm eliminates or prunes all candidate item sets whose support count is less than minsup threshold value given.
Step 7	Finally algorithm terminates when there are no new frequent item sets generated.

Apriori algorithm traverses the item set one level at a time, from frequent 1-itemsets to the maximum size of frequent itemsets.Secondly, new candidate item sets are generated from the frequent item sets found in the previous iterations and support of each is then counted and checked against the minimum threshold values [13].

IV. RESULTS AND DISCUSSION

In this paper, dataset consisting of different course combinations(X) and preferable courses(Y) shown in Table I are fed into WEKA tool where Apriori Association Rule Mining Algorithm is applied.

TABLE IV. APRIORI Associator Output

Minimum support: 0.1 (1 instances)
Minimum metric <confidence>: 0.9
Number of cycles performed: 18
Generated sets of large item sets:
Size of set of large item sets L (1): 20
Size of set of large item sets L (2): 13

Table IV shows that minimum support taken for the dataset is 0.1 and confidence is 0.9.Number of cycles performed on the dataset is 18 and number of frequent 1-Itemset and 2 item sets are 20 and 13.

TABLE V. Best Rules Found By APRIORI

Course Combination(X)=Java,J2EE 1	==> Preferable Course(Y)=Android 1	conf:(1)
Course Combination(X)=Java,J2EE,HTML 1	==> Preferable Course(Y)=Android 1	conf:(1)
Course Combination(X)=HTML,Javascript 1	==> Preferable Course(Y)=PHP 1	conf:(1)
Preferable Course(Y) = Asp.Net 1	==> Courses Combination(X)=C,C++ 1	conf:(1)
Course Combination(X)=J2EE,Java 1	==> Preferable Course(Y)=Android 1	conf:(1)
Course Combination(X)=C,C++,VB.Net 1	==> Preferable Course(Y)=Java 1	conf:(1)
Course Combination(X)=HTML 1	==> Preferable Course(Y)=PHP 1	conf:(1)
Course Combination(X)=HTML,Asp.net 1	==> Preferable Course(Y)=PHP 1	conf:(1)
Preferable Course(Y)=C++ 1	==> Courses Combination(X)=C 1	conf:(1)
Course Combination(X)=C 1	==> Preferable Course(Y)=C++ 1	conf:(1)

Best rules generated by Apriori and Predictive Apriori Associator in Weka tool on dataset in Table II are shown in Table V and VI.Table V shows the preferable courses for students based on their course combinations.E.g: "Android" is the preferable course for industrial training for those students who have done java and J2EE in their semesters.

TABLE VI. Best Rules Found By Predictive APRIORI

Course Combination(X)=C,C++ 3 ==> Preferable Course(Y)=Java 2 acc:(0.47888)
Preferable Course(Y)=Java 3 ==> Courses Combination(X)=C,C++ 2 acc:(0.47888)
Course Combination(X)=Java,J2EE 3 ==> Preferable Course(Y)=Android 3 acc:(0.47888)

Predictive Apriori Algorithm uses pruning strategy where it searches for the best rules and highly accurate rules which are included by less accurate ones remain part of the output. Predictive Apriori uses an increasing support values and is able to mine a high quality set of association rules. Predictive Apriori algorithm performs well when it is used to generate a small set of rules [11].

V. CONCLUSION

In this paper we have discussed about ARM and its usage in Educational field. Using ARM technique, students seek help in choosing right course for their industrial trainings based on different course combinations.ARM is used to find associations between frequently occurring variables. Association rules are generated based on the frequent variables in datasets. Apriori is the algorithm used for mining of frequent patterns from the transaction database. Rules discovered using Apriori Algorithm not only help students but also help teachers to find student's interest towards industry oriented courses in an e-learning environment and enhances the effectiveness of academic planning, decision-making. In future, Association Rule Mining would be helpful in finding rules related to industry demanding courses to be introduced into syllabi.

REFERENCES

[1] Ruijuan Hu, *Medical Data Mining Based on Association Rules*, Computer and Information Science, ISSN 1913-8989 E-ISSN 1913- 8997, *Vol. 3, No. 4;* November 2010.

[2] B. Liu and C.K. Wong, " *Improving an association rule based classifier",* journal In Principles of Data Mining and Knowledge Discovery, p. 504–509, 2000.

[3] Enrique García, Cristobal Romero, Sebastián Ventura, Carlos de Castro, *"A collaborative educational association rule mining tool"*, Internet and Higher Education 14 (2011) 77–88, doi:10.1016/j.iheduc.2010.07.006.

[4] Dion H. Goh, Rebecca P. Ang,*"An introduction to association rule mining: An application in counseling and help-seeking behavior of adolescents"*, Behavior Research Methods 2007, 39 (2), 259-266.

[5] Pirjo Moen, "*Data mining methods*", Spring 2005, referred from http://www.cs.helsinki.fi/u/ronkaine/tilome/luentomateriaali/TiLoMe-170105.pdf.

[6] P. Rajendran, M.Madheswaran,"*Hybrid Medical Image Classification Using Association Rule Mining with Decision Tree Algorithm*", Journal of Computing, ISSN 2151-9617, *Vol 2, Issue 1*, January 2010.

[7] Mirela Danubianu, Stefan Gheorghe Pentiuc, Iolanda Tobolcea,"*Mining Association Rules Inside a Relational Database – A Case Study*",ICCGI 2011 : The Sixth International Multi-Conference on Computing in the Global Information Technology, Copyright (c) IARIA,ISBN: 978-1-61208-139-7, 2011.

[8] Varun Kumar, Anupama Chadha,"*Mining Association Rules in Student's Assessment Data*", IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0814, *Vol. 9, Issue 5*, No. 3, September 2012.

[9] Oladipupo, I.C O.O., Oyelade O.J.,"*Knowledge Discovery from Students' Result Repository: Association Rule Mining Approach*", International Journal of Computer Science & Security (IJCSS), *Vol 4: Issue (2).*

[10] Paresh Tanna, Yogesh Ghodasara,"*Using Apriori with WEKA for Frequent Pattern Mining*", International Journal of Engineering Trends and Technology (IJETT), ISSN: 2231-5381, *Vol 12 No.3*, Jun 2014.

[11] Stefan Mutter, Mark Hall, Eibe Frank, "*Using Classification to Evaluate the Output of Confidence-Based Association Rule Mining*".

[12] K.S. Adewole, A.G. Akintola & A.R. Ajiboye,"*Frequent Pattern and Association Rule Mining from Inventory Database Using Apriori Algorithm*", African Journal of Computing & ICT, ISSN 2006-1781, *Vol 7. No. 3* - September, 2014.

[13] Tan, Pang-Ning, Vipin Kumar, "Chapter 6. *Association Analysis: Basic Concepts and Algorithms."* Introduction to Data Mining. Addison-Wesley. ISBN321321367, 2005

A MULTIPATH ROUTING PROTOCOL FOR COGNITIVE RADIO AD HOC NETWORKS

Abinaya.J[1], Gayathri.T[2] and Saranya.N[3]

[1,2,3] *ECE, SNS College of Technology/M.E(CS), Coimbatore, Tamil nadu, (India)*

ABSTRACT

Multihop routing is the advanced technology in wireless Networks. Multipath routing protocols for MANET are deemed superior over conventional single-path routing as the former to reduce end to end delay, increase consistency and provide toughness. Quality of Service (QoS) is an essential feature of networks. One of the main problems in Ad-hoc networking is the delivery of data packets to the nodes where the topology is not predetermined. Hence, implemented route stability based multipath QoS (AOMDV) protocol to support higher throughput and reduced delay, in real time application networks. The simulation result outperforms AODV Protocol with a throughput of 87.5% and delay of about 2.5% for 20 nodes.

Keywords: Multihop, MANET, QoS, Throughput

I. INTRODUCTION

Cognitive Radio (CR) technology is to enhance the spectrum utilization by enabling unlicensed users to exploit the spectrum in an opportunistic manner. Cognitive Radio is a transceiver which automatically detects the available channels in wireless spectrum. It is a key technology to realize Dynamic Spectrum Access (DSA) that enables an unlicensed user to adaptively adjust its operating parameters and exploit the spectrum which is unused by licensed users in an opportunistic manner. A cognitive network is an opportunistic network. Spectrum opportunity deals with the usage of an available (free) channel that is a part of the spectrum which is not currently used by primary users.

A cognitive radio is a SDR (Software Defined Radio) with a cognitive engine brain. Cognitive radio is considered as a goal towards which a software-defined radio platform should evolve a fully reconfigurable wireless transceiver which automatically adapts its communication parameters to network and user demands. Cellular network bands are overloaded in most parts of the world, but other frequency bands (such as military, amateur radio and paging frequencies) are insufficiently utilized. Moreover, fixed spectrum allocation prevents rarely used frequencies (those assigned to specific services) from life form used, even while any unlicensed users would not cause noticeable interference to the assigned service. Thus it allows unlicensed users in licensed bands if unlicensed users would not root any intrusion to licensed users. These initiatives have alert cognitive-radio research on dynamic spectrum access.

Cognitive radio and ad-hoc networks implement proactive spectrum handoff protocol. The first forwarding system before proactive spectrum handoff protocol was reactive spectrum handoff protocol. In reactive spectrum handoff protocol unlicensed users are temporary visitors to the licensed spectrum; they are required to

vacate the spectrum when a licensed user reclaims it. When the temporary visitors fail to vacate the spectrum collision might occur which leads to low throughput. But however reactive spectrum handoff protocol has a fundamental limitation that is limited by allocating a spectrum channel to the secondary user which is not used by the secondary user. The collisions and low throughput are the most common case of the failures in the reactive spectrum handoff protocol, which is overcome by the proactive spectrum handoff protocol. Thus, it avoids collisions and increases the throughput.

II. PROACTIVE SPECTRUM HANDOFF APPROACH

2.1 Introduction

Cognitive radio (CR) can improve spectrum efficiency through intelligent spectrum management technologies by allowing secondary users to temporarily access primary users' unutilized licensed spectrum. In order to enhance spectrum management, CR systems require many capabilities such as spectrum mobility (or called spectrum handoff). Spectrum handoff occurs when the high-priority primary users appear at its licensed band occupied by the secondary users. Spectrum handoff procedures aim to help the secondary users to vacate the occupied licensed spectrum and find suitable target channel to resume the unfinished transmission .In general, according to the target channel decision methods, spectrum handoff can be categorized into two mechanisms. They are proactive-decision spectrum handoff and reactive spectrum handoff. Proactive decision spectrum handoff which makes the target channels for spectrum handoff ready before data transmission according to the long-term observation. Reactive decision spectrum handoff determines the target channel according to the results from on-demand wideband sensing. Compared to the reactive-decision spectrum handoff, the proactive-decision spectrum handoff may be able to reduce handoff delay because the time-consuming wideband sensing is not required. Furthermore, it is easier to let both transmitter and receiver have a consensus on their target channel for the proactive-decision spectrum handoff than for the reactive decision spectrum handoff. Nevertheless, when the spectrum handoff process is initiated, the proactive-decision spectrum handoff needs to resolve the issue that the pre-selected target channel may no longer be available. Hence, one challenge for the proactive-decision handoff is to determine the optimal target channel sequences to minimize total service time.

2.2 Objective

The main aim of this project is to make the unlicensed users to use the licensed spectrum in an efficient way and to vacate a channel before a licensed user utilizes it, to avoid unwanted interference & to achieve higher packet delivery rate and there is proven increase in the throughput.

2.3 Spectrum Handoff in Cognitive Radio Network

Related work on spectrum handoffs in CR networks falls into two categories based on the moment when SUs carry out spectrum handoffs. One approach is that SUs perform spectrum switching and Radio Frequency (RF) front-end reconfiguration after detecting a PU, namely the reactive approach. Although the concept of this approach is intuitive, there is a non-negligible sensing and reconfiguration delay which causes unavoidable disruptions to both the PU and the SU transmissions.

Another approach is that SUs predict the future channel availability status and perform spectrum switching and RF reconfiguration before a PU occupies the channel based on observed channel usage statistics, namely the proactive approach. This approach can dramatically reduce the collisions between SUs and PUs by letting SUs vacate channels before a PU reclaims the channel. In the proactive approach, a predictive model for dynamic spectrum access based on the past channel usage history is proposed in. A cyclostationary detection and Hidden Markov Models for predicting the channel idle times are proposed in a binary time series for the spectrum occupancy characterization and prediction is proposed. In a novel spectrum handoff scheme called voluntary spectrum handoff is proposed to minimize SU disruption periods during spectrum handoff .The error prediction of the channel usage is considered in designing an intelligent dynamic spectrum access mechanism. The experimental cognitive radio test bed is presented. It uses sensing and channel usage prediction to exploit temporal white space between primary WLAN transmissions.

2.4 Channel Selection in CR Networks

Even though the channel allocation issue has been well studied in traditional wireless networks (e.g., cellular networks and Wireless Local Area Networks (WLANs)), channel allocation in CR networks, especially in a spectrum handoff scenario, and still lacks sufficient research. When SUs perform spectrum handoffs, a well-designed channel selection method is required to provide fairness to all SUs as well as to avoid multiple SUs to select the same channel at the same time. Currently, the channel selection issue in a multi-user CR network is investigated mainly using game theoretic approaches. Furthermore, most of the prior work on channel allocation in spectrum handoffs only considers a two secondary user scenario, where a SU greedily selects the channel which either results in the minimum service time or has the highest probability of being idle. Only one pair of SUs is considered and the channel selection issue is ignored. However, if multiple SUs perform spectrum handoffs at the same time, these channel selection methods will cause definite collisions among SUs. Hence, the channel selection method aiming to prevent collisions among SUs in a multisecondary- user spectrum handoff scenario is ignored in the prior work.

2.5 Analytical Model for Spectrum Handoff in CR Networks

An analytical model is of great importance for performance analysis because it can provide useful insights into the operation of spectrum handoffs. However, there have been limited studies on the performance analysis of spectrum handoffs in CR networks using analytical models. The performance analysis of all prior works on spectrum handoff is simulation based with the exception of that a pre emptive resume priority queuing model is proposed to analyze the total service time of SU communications for proactive and reactive-decision spectrum handoffs. However, only one pair of SUs is considered in a network, while the interference and interactions among SUs are ignored, which greatly affect the performance of the network. In all the above proposals, a common and severe limitation is that the authors assume that the detection of PUs is perfect *i.e.*, a SU transmitting pair can immediately perform channel switching if a PU is detected to appear on the current channel, thus the overlapping of SU and PU transmissions is negligible. However, since the power of a transmitted signal is much higher than the power of the received signal in wireless medium due to path loss, instantaneous collision detection is not possible for wireless communications. Thus, even if only a portion of a

packet collides with another transmission, the whole packet is wasted and needs to be retransmitted. Without considering the retransmission, the performance conclusion may be inaccurate, especially in wireless communications.

2.6 The Proposed Distributed Channel Selection Scheme

The performance of the proposed channel selection scheme is investigated and compared it with the following three different channel selection methods under the proposed proactive spectrum handoff scenario using the single rendezvous coordination scheme.

Random channel selection: A SU randomly chooses a channel from its predicted available channels.

***Greedy channel selection*:** In this method, only one pair of SUs is considered in the network. The SUs can obtain all the channel usage information and predict the service time on each channel. Thus, when a spectrum handoff occurs, a SU selects a pre-determined channel that leads to the minimum service time.

Local bargaining: In this method, SUs form a local group to achieve a collision free channel assignment. To make an agreement among SUs, a four-way handshake is needed between the neighbours *i.e.*, request, acknowledgment, action, acknowledgment. Since one of the SUs is the initiating node which serves as a group header, the total number of control messages exchanged is 2*N*LB, where *N*LB is the number of SUs needed to perform spectrum handoffs. Since for channel selection schemes, reducing the number of collisions among SUs is the primary goal, consider the SU throughput, average SU service time, collisions among SUs, and average spectrum handoff delay as the performance metrics.

2.7 Advantage

1) A distributed channel selection scheme to eliminate collisions among unlicensed users in a multiuser spectrum handoff so that, there is no interference or collisions.
2) As there are no collisions the proactive spectrum can achieve high throughput value and higher packet delivery.
3) Due the spectrum handoff, packet loss is greatly reduced.
4) Compared to reactive spectrum the quality of service is improved

III. RESULTS & DISCUSSION

Implementation is done by using Ns-2 software.

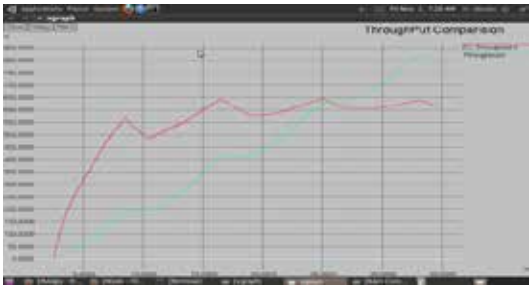


Fig 3.1 Graph Representing Throughput in Wireless Networks

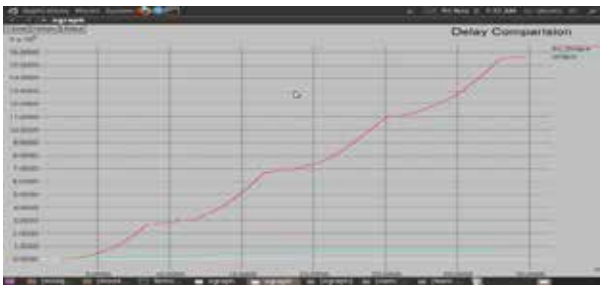


Fig 3.2 Graph Representing Delay in Wireless Networks

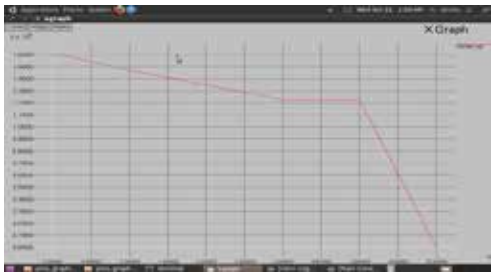


Fig 3.3 Graph representing delay in CR Technology

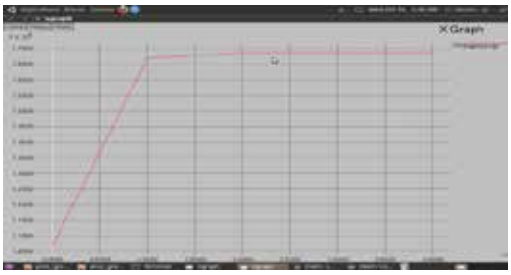


Fig 3.4 Graph representing Throughput in CR Technology

DISCUSSION

Fig 3.1, 3.2 shows the performance of the existing work in terms of congestion detection & avoidance. In Fig 3.1 the existing work shows that, as the transmission rate increases throughput also initially increases and then drops due to collision in the network, whereas in congestion detection & avoidance, it initially increases and then remains constant as it avoids collision .Thus it achieves higher throughput of about 78.6% .In Fig 3.2 the existing work shows that as the number of user increases, the delay also increases and it reaches infinity, whereas in congestion detection & avoidance it is noted that delay is slightly increased and remains constant wherever the probability of maximum collision is more .Thus delay is decreased by 5.41%. Fig 3.3 and 3.4 shows the performance of different number of secondary users. In Fig 3.3 CR technology shows that as the number of SUs increases the throughput also increases and then remains constant because of the maximum utilization of unused spectrum. It achieves a throughput of about 85%. In Fig 3.4 it shows as the number of users increases delay is reduced to about 3.5%. From Table 3.1 The result analysis shows that comparison between wireless network and CR technology .There are various drawbacks in the wireless networks which includes low throughput and more delay. On analyzing the cognitive radio technology, unused spectrum utilization is more, collision avoidance and interference is less. Thus high throughput and packet delivery is achieved.

IV CONCLUSION

In cognitive radio technology interference and collision avoidance is explained. Proactive spectrum handoff protocol triggers the unlicensed users to vacate the channel before the licensed user utilizes it. Cognitive Radio can achieve higher packet delivery and maximum throughput.

V FUTURE WORK

Channel sensing in Cognitive Radio can be carried out by using waveform based sensing.

REFERENCES

[1]. Bahl. P, Chandra. R and Dunagan. J, 2004 'SSCH: Slotted Seeded Channel Hopping for Capacity Improvement in IEEE 802.11 Ad-Hoc Wireless Networks,' Proc. ACM MobiCom, pp. 216-230.

[2]. Geirhofer.S, Tong. L and Sadler. B, 2008 'Cognitive Medium Access: Constraining Interference Based on Experimental Models, IEEE J. Selected Area in Comm. (JSAC), vol. 26, no. 1, pp. 95-105.

[3]. Huang. S, Liu. X and Ding. Z, 2009 'Optimal Transmission Strategies for Dynamic Spectrum Access in Cognitive Radio Networks,' IEEE Trans. Mobile Computing, vol. 8, no. 12, pp. 1636-1648.

[4]. Kondareddy.Y.R and Agrawal. P, 2008'Synchronized MAC Protocol for Multi-Hop Cognitive Radio Networks,' Proc. IEEE Int. Conf. Comm. (ICC), pp. 3198-3202.

[5]. Mishra.S, Sahai.A and Brodersen.R, 2006 'Cooperative Sensing among Cognitive Radios,' Proc. IEEE Int. Conf. Comm. (ICC),pp. 1658-1663.

[6]. Mo.J, So.H.-S.W and Walrand.J, 2008 'Comparison of Multichannel MAC Protocols,' IEEE Trans. Mobile Computing, vol. 7, no. 1, pp. 50-65.

[7]. Qu.D, Ding.J, Jiang.T and Sun.X, 2011 'Detection of Non-Contiguous OFDM Symbols for Cognitive Radio Systems Without Out-of-Band Spectrum Synchronization,' IEEE Trans. Wireless Comm., vol. 10, no. 2, pp. 693-701.

[8]. Qu.D, Wang.Z and Jiang.T, 2010'Extended Active Interference Cancellation for Sidelobe Suppression in Cognitive Radio OFDM Systems with Cyclic Prefix,' IEEE Trans. Vehicular Technology, vol. 59, no. 4, pp. 1689-1695.

[9]. So. H.W and Walrand. J, 2007'McMAC: A Multi-Channel MAC Proposal for Ad-Hoc Wireless Networks,' Proc. IEEE Wireless Comm. and Networking Conf. (WCNC)

[10]. Song. Y and Xie .J, 2009 'Optimal Power Control for Concurrent Transmissions of Location-Aware Mobile Cognitive Radio Ad-Hoc Networks,' Proc. IEEE GlobeCom, pp. 1-6

DESIGN AND IMPLEMENTATION OF A LOW VOLTAGE LOW POWER DOUBLE TAIL COMPARATOR

[1]C.Hamsaveni, [2]R.Ramya

[1]PG Scholar, [2]PG Scholar, Department of ECE, Hindusthan Institute Of Technology, Coimbatore.

ABSTRACT

Comparators are the basic elements for designing the modern analog and mixed signal systems. The speed and area is main factors for high speed applications. Various types of dynamic double tail comparators are compared in terms of Delay, Area, Power, Glitches, Speed and average time. The accuracy of comparators it mainly defined by its power consumption and speed. The comparators are mainly achieving the overall higher performance of ADC. The High speed comparators suffer from low voltage supply. Threshold voltage of the device is not scaled at the same time, as the supply voltage of the device. In modern CMOS technology the double tail comparator is designed by a using the dynamic method, it mainly reduces the power and voltage. The analytical expression method it can obtain an intuition about the contributors, comparator delay and explore the trade-off dynamic comparator design.

Keyword: Double Tail comparator, ADC, Dynamic comparator, Glitches

I INTRODUCTION

Comparators have essential influence on the overall performance in high speed analog to digital convertors (ADCs). In wide-ranging a comparator is a device, which compares two currents or voltages and produces the digital output based on the comparison. Since comparators are usually not used with the feedback there is not compensation so neither the area reduction or speed reduction value is invited. Comparators are known as 1-bit analog to digital converter and for that reason they are mostly used in large quantity in A/D converter Dynamic comparators are widely used in the design of high speed ADCs. Due to speed, low power consumption, high input impedance and full swing output, the dynamic latched comparators are very attractive for many kinds of applications such as high speed analog to digital converters (ADCs), memory sense amplifiers. Increasing packing densities coupled with faster clock frequencies has forced the issue of heat removal and power dissipation to the forefront of virtually every mainstream design application under the SUR. And the problem is predicted to continue to be a major challenge in the coming decade as we approach Giga Scale Integration (GSI) [1]. Analogue to digital conveners are one of the main building blocks of most portable electronic equipments, such as cell phones, electronics products. They increasing demand of longer battery life time of portable equipments has forced circuit designers to use lower supply

voltages. However the supply voltage is lowered the performance of analogue circuits is degraded and the design of low voltage analogue Circuits

This technique is very suitable for very-low power clocked and continuous time circuits such as level shifters, Op-amp and comparators. Design of a 10-bit supply boosted (SB) SAR ADC is presented as an example of the technique. Voltage design techniques such as clock boosting were also used. A unique supply and clock booster was designed as integral part of new supply boosted comparator. Input common mode range of SB comparator was extended by using supply boosted level shifter circuits [6]. Among the key performance metrics of a dynamic latch used in a voltage comparator is its input referred offset voltage. Relevant effects that contribute to the offset can be divided into static and dynamic components. The most commonly discussed source of static offset stems from threshold voltage mismatch in the constituent transistors. Two simple equations for predicting the offset were derived and compared against simulation data [7].

The degeneration resistors are the latching pair and it's to reduce transistor charging time for regeneration. Charging time, they allowing more time for regeneration. The introduction method consists of the emitter degeneration resistors in the latching pair. The degeneration resistors reduce the transistor charging time, providing more time for the critical process of regeneration. As the latching pair is isolated from the input nodes degenerates still improves the sensitivity when a preamplifier is used [8]. To overcome the challenges associated with to reduce the supply voltage, a double tail latched comparator with a variable capacitance, calibration technique they using a metal oxide metal capacitors is implemented. An all-digital time domain delay interpolation technique further enhances the resolution with very little additional power consumption [9].

II CONVENTIONAL DYNAMIC COMPARATOR

The double tail comparator achieves the better performance and the double tail comparator and the architecture it mainly used in the better performance used in the low voltage applications. The comparator designed based on double tail architecture. The main idea of this method is to increase ΔVfn/*fp* is to increase the latch regeneration speed. The main operation of the comparator is during reset phase CLK = 0, Mtail1 and Mtail2 is off, to avoiding these static power, M3 and M4 switches pulls both fn and fp nodes to VDD. Hence the transistor Mc1 and Mc2 are cut off, intermediate stage transistors MR1 and MR2 is reset both latches outputs to ground. During decision making phase CLK = VDD. Mtail1 and Mtail2 are on transistors M3 and M4 turn off. Furthermore, at the beginning of the phase, the control transistors are still off. Thus, fn and fp start to drop with different rates according to the input voltages. The second term, *t*latch, is the latching delay of two cross coupled inverters. It is assumed that a voltage swing of *V*out = *V*DD/2 has to be obtained from an initial output voltage difference V0 at the falling output. This is a self biasing differential amplifier. An inverter was added at the output of the amplifier as an additional gain stage, to isolate any load capacitance from the self biasing differential amplifier.

The size of M1 and M2 are set by considering the differential amplifier's transconductance and the input capacitance. The transconductance sets the gain of the stages, while the input capacitance of the comparator is determined by the size M1 and M2. Similar to the conventional dynamic comparator, the delay of this comparator comprises two main parts, t0 and tlatch. The delay t0 represents the capacitive charging of the load capacitance CL

out (at the latch stage output nodes, Outn and Outp) until the first n-channel transistor (M9/M10) turns on, after which the latch regeneration starts; thus t0 is obtained where IB1 is the drain current of the M9 and approximately equal to the half of the tail current. Thus, it can be concluded that two main parameters which influence the initial output differential voltage and thereby the latch regeneration time are the transconductance of the intermediate stage transistors (*g*mR1,2) and the voltage difference at the first stage outputs (fn and fp) at time *t*0.

III PROPOSED DOUBLE TAIL COMPARATOR

To achieve the better performance of double tail architecture in low voltage applications, the proposed method comparator is designed based on the double-tail structure

Operation of Proposed Comparator

1. Voltage is sense at the second stage input and the second stage latch regenerate output voltage Reset Phase: Clk = 0, Mtail1and Mtail2 OFF. For this process static power is avoided. np and nf nodes to VDD. Latches to be Ground.
2. Decision making phase: Clk = VDD, Mtail1 and Mtail2 are ON, M3 and M4 OFF.

During reset phase clk=0, Mtail1 (M3) &Mtail2 (M20) are OFF, M10&M13will pull both fn & fp nodes to VDD. Hence MC (M11) & MC (M12) are cut off, M6 M9 are discharge to output nodes to VSS. During an decision making phase clk =VDD,Mtail1(M3)&Mtail2(M20) are ON, transistor M10&M13 will OFF and fn & fp nodes are start drop with different rates according to input voltage. VINP>VINN means fn is faster than fp, M15 transistor provide more current thanM14.MC (M11) is turn on, fp node pulling back to VDD MC (M12) remains OFF, fn node discharged. Offset will low and delay reduced. Parallel connected dynamic latch is used as load of first stage to increase voltage difference due to cascade connection delay will more compare to parallel connection. The latch of this first stage start regenerating depending on the input differential voltage (Vin1, Vin2), producing a large difference voltage. This difference Out1 and Out2.As fast sensing it is exploiting less time to produce output when compare to previous work. It consumes less power compared to conventional one. As the way delay has reduced.

IV EXPERIMENTAL RESULTS

Existing Model

In order to compare the proposed comparator with the conventional and double tail dynamic comparator all circuits have been simulated in a 130nm CMOS technology the post layout simulation have been simulated in Tanner EDA which is used to calculate the area of the conventional dynamic comparator as shown in Fig 1, Double tail dynamic comparator as in Fig 3 and proposed double tail dynamic comparator.

Circuit Diagram

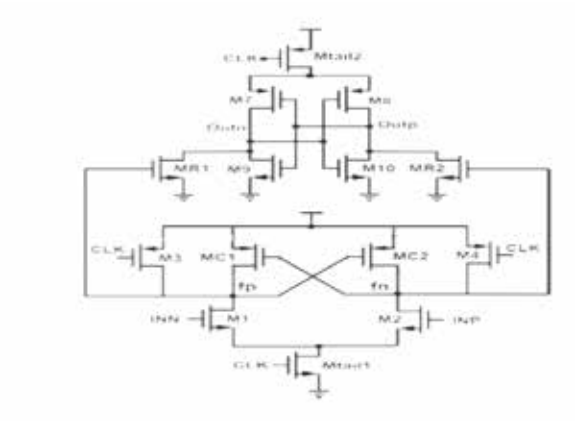


Fig .1 Existing Dynamic Comparator

Due to the fact that parasitic capacitances of input transistors do not directly affect the switching speed of the output nodes, it is possible to design large input transistor to minimize the offset. The disadvantage, on the other hand, is the fact that due to several stacked transistors, a sufficiently high supply voltage is needed for a proper delay time. The reason is that, at the beginning of the decision, only transistors *M*3 and *M*4 of the latch contribute to the positive feedback until the voltage level of one output node has dropped below a level small enough to turn on transistors *M*5 or *M*6 to start complete regeneration.

Graph Output

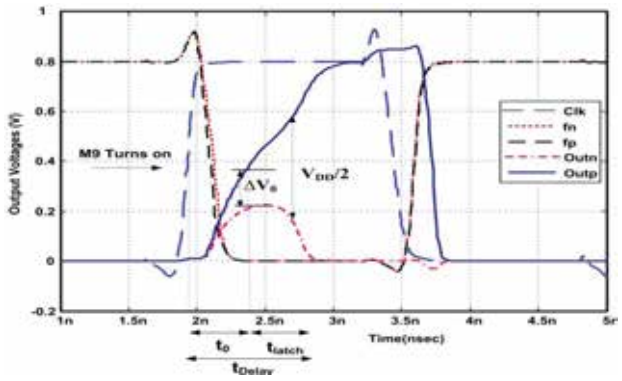


Fig.2 Energy diagram of existing system.

Proposed Method

As long as fn continues falling, the corresponding PMOS control transistor (*M*c1 in this case) starts to turn on, pulling fp node back to the *V*DD; so another control transistor (*M*c2) remains off, allowing fn to be discharged completely. In other words, unlike conventional double-tail dynamic comparator, in which *V*fn/fp is just a function of input transistor transconductance and input voltage difference in the proposed structure as soon as the comparator detects that for instance node fn discharges faster, a PMOS transistor (*M*c1) turns on, pulling the other node fp back to the *V*DD.

Circuit

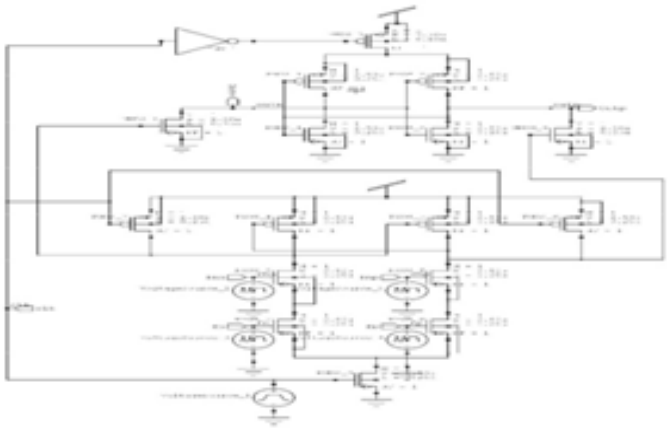


Fig 3 Proposed Circuit

Therefore by the time passing, the difference between fn and fp (*V*fn/fp) increases in an exponential manner, leading to the reduction of latch regeneration time.

It is evident that the double-tail topology can operate faster and can be used in lower supply voltages, while consuming nearly the same power as the conventional dynamic comparator. The case is even much better for the proposed comparator when compared to the conventional double-tail topology.

Parsing	0.10 seconds
Setup	0.01 seconds
DC operating point	0.00 seconds
Transient Analysis	1.14 seconds
Overhead	2.01 seconds
Total	3.26 seconds

Simulation Graph

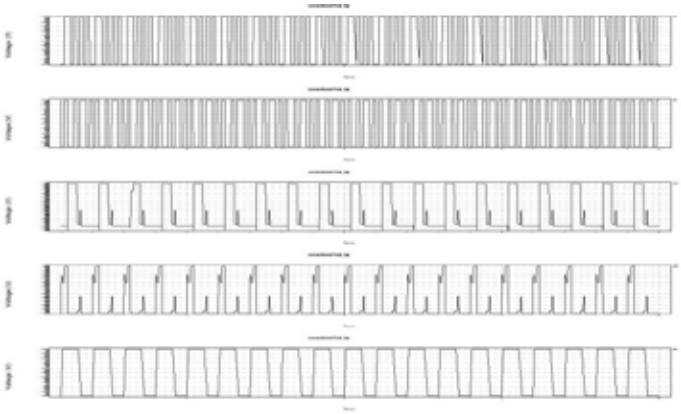


Fig.4 Proposed Output

V CONCLUSION

This work presents that comprehensive delay analysis for clocked dynamic comparators. Two common structures of conventional dynamic comparator and conventional double- tail dynamic comparators have been analyzed. A new dynamic comparator with low-voltage low-power capability has been proposed in order to improve the performance of the comparator and also reduces the delay. The area estimation is evaluated using post layout simulation with the help of micro wind simulator.

REFERENCES

[1] B. Goll and H. Zimmermann, "A comparator with reduced delay time in 65-nm CMOS for supply voltages down to 0.65," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 56, no. 11, pp. 810–814, Nov. 2009.

[2] S. U. Ay, "A sub-1 volt 10-bit supply boosted SAR ADC design in standard CMOS," Int. J. Analog Integr. Circuits Signal Process., vol. 66, no. 2, pp. 213–221, Feb. 2011.

[3] A. Mesgarani, M. N. Alam, F. Z. Nelson, and S. U. Ay, "Supply boosting technique for designing very low-voltage mixed-signal circuits in standard CMOS," in Proc. IEEE Int. Midwest Symp. Circuits Syst. Dig. Tech. Papers, Aug. 2010, pp. 893–896.

[4] B. J. Blalock, "Body-driving as a Low-Voltage Analog Design Technique for CMOS technology," in Proc. IEEE Southwest Symp. Mixed-Signal Design, Feb. 2000, pp. 113–118.

[5] M. Maymandi-Nejad and M. Sachdev, "1-bit quantiser with rail to rail input range for sub-1V __ modulators," IEEE Electron. Lett., vol. 39, no. 12, pp. 894–895, Jan. 2003.

[6] Y. Okaniwa, H. Tamura, M. Kibune, D. Yamazaki, T.-S. Cheung, J. Ogawa, N. Tzartzanis, W. W. Walker, and T. Kuroda, "A 40Gb/ s CMOS clocked comparator with bandwidth modulation technique," IEEE J. Solid-State Circuits, vol. 40, no. 8, pp. 1680–1687, Aug. 2005.

[7] B. Goll and H. Zimmermann, "A 0.12 μm CMOS comparator requiring 0.5V at 600MHz and 1.5V at 6 GHz," in Proc. IEEE Int. Solid-State Circuits Conf., Dig. Tech. Papers, Feb. 2007, pp. 316–317.

[8] B. Goll and H. Zimmermann, "A 65nm CMOS comparator with modified latch to achieve 7GHz/1.3mW at 1.2V and 700MHz/47μW at 0.6V," in Proc. IEEE Int. Solid-State Circuits Conf. Dig. Tech. Papers, Feb. 2009, pp. 328–329.

[9] B. Goll and H. Zimmermann, "Low-power 600MHz comparator for 0.5 V supply voltage in 0.12 μm CMOS," IEEE Electron. Lett., vol. 43, no. 7, pp. 388–390, Mar. 2007.

[10] D. Shinkel, E. Mensink, E. Klumperink, E. van Tuijl, and B. Nauta, "A double-tail latch-type voltage sense amplifier with 18ps Setup+Hold time," in Proc. IEEE Int. Solid-State Circuits Conf., Dig. Tech. Papers, Feb. 2007, pp. 314–315.

[11] P. Nuzzo, F. D. Bernardinis, P. Terreni, and G. Van der Plas, "Noise analysis of regenerative comparators for reconfigurable ADC architectures," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 55, no. 6, pp. 1441–1454, Jul. 2008.

[12] A. Nikoozadeh and B. Murmann, "An analysis of latched comparator offset due to load capacitor mismatch," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 53, no. 12, pp. 1398–1402, Dec. 2006.

[13] S. Babayan- Mashhadi and R. Lotfi, "An offset cancellation technique for comparators using body-voltage trimming," Int. J. Analog Integr. Circuits Signal Process., vol. 73, no. 3, pp. 673–682, Dec. 2012.

[14] J. He, S. Zhan, D. Chen, and R. J. Geiger, "Analyses of static and dynamic random offset voltages in dynamic comparators," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 56, no. 5, pp. 911–919, May 2009.

RECENT ADVANCES ON Sn–Zn SOLDERS WITH ALLOYING ELEMENTS: REVIEW

Harpreet Singh

Mechanical Engineering, Y.I.E.T Gadholi, (India)

ABSTRACT

Sn-9Zn Solder have been considered as one of the more appropriate lead free solder since it can easily replace Sn-Pb eutectic solder alloy without increasing its eutectic temperature. However there are still some problems related to wetting and mechanical properties to be resolved. In order to improve these properties of Sn-Zn Solder alloy a small amount of alloying elements (rare earths Pr, Nd and Sb) added into Sn-Zn solder alloys were studied by many researchers. For example, a small addition of Pr and Nd can improve the wettability and mechanical properties of Sn-Zn solder alloy. This paper summarizes the effects of alloying elements on the wetability, mechanical properties, microstructure and intermetallic compounds layer of Sn-Zn solder alloy.

Keywords: Intermetallic Compound, Lead Free Solder, Mechanical Properties, Microstructure, Wetability

I INTRODUCTION

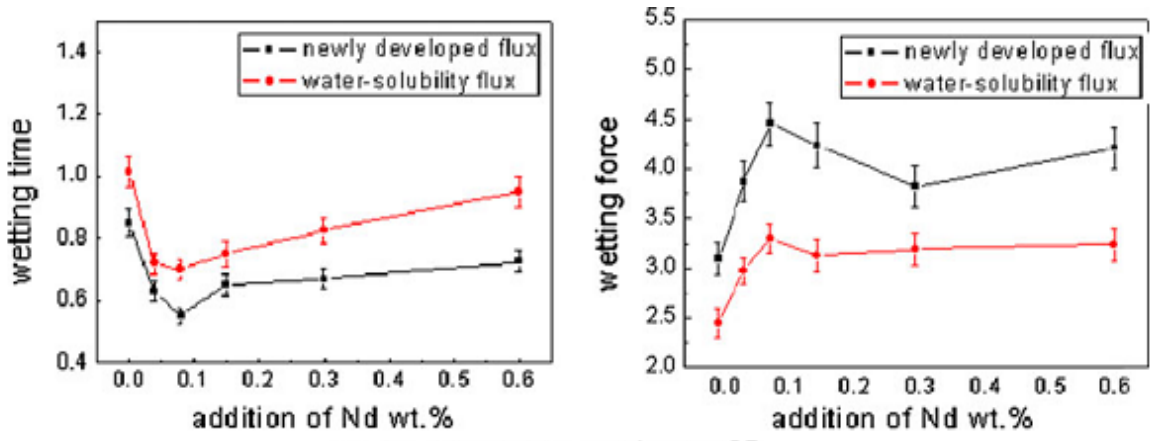
Due to the implementation of the directive on Waste Electrical and Electronic Equipment (WEEE) and the directive on the Restriction of the Use of Hazardous Substances in Electrical and Electronic Equipment (RoHS Directive) [1–3], thus, an urgent necessity exists for more appropriate candidate for the traditional Sn–Pb solder alloy. Furthermore, it is more important that the mechanical and physical properties of the candidate are comparable or even better then Sn-Zn solder alloy [4]. Among lot of lead free solder, Sn-Ag-Cu alloy has been drawn special focus and regarded as most promising lead free candidate for the traditional Sn-Pb solder alloy [5, 6]. But the Sn-Ag-Cu solder alloys have higher eutectic temperature then Sn-Pb solder alloy [7]. While Sn-Zn solder alloy gain more attention as the eutectic temperature is 20^0C lower then Sn-Ag-Cu system [8]. But its poor wettability limited its use in electronic industry. The main reason for this is Zn which easily react with oxygen and form ZnO which decrease its wettability. Basically, there are two ways to increase the wettability of Sn-Zn solder alloy: one is to develop a new flux which is fit for Sn-Zn solder; and the other is to develop Sn-Zn solder alloy doped with additives [9]. The wettability of Sn–9Zn–X can be obviously improved in N_2 atmospheres. It is also found that Sn–9Zn–X lead-free solders show preferable wettability with ZnCl2–NH4Cl flux, even better than that of Sn–3.5Ag–0.5Cu solder under same condition. In addition, rare earths (RE), Cu, Bi, In can effectively improve the wettability, mechanical properties, oxidation resistance of eutectic Sn–Zn alloys [10, 11].

In order to enhance the properties of Sn–Zn solder, such as wettability, mechanical properties, a small amount of alloying elements were selected by lots of researchers as alloys addition into these alloys. For example, surface tension of Sn–Zn solder alloy can be reduced with addition of Bi, however wettability of Sn–Zn–Bi solders

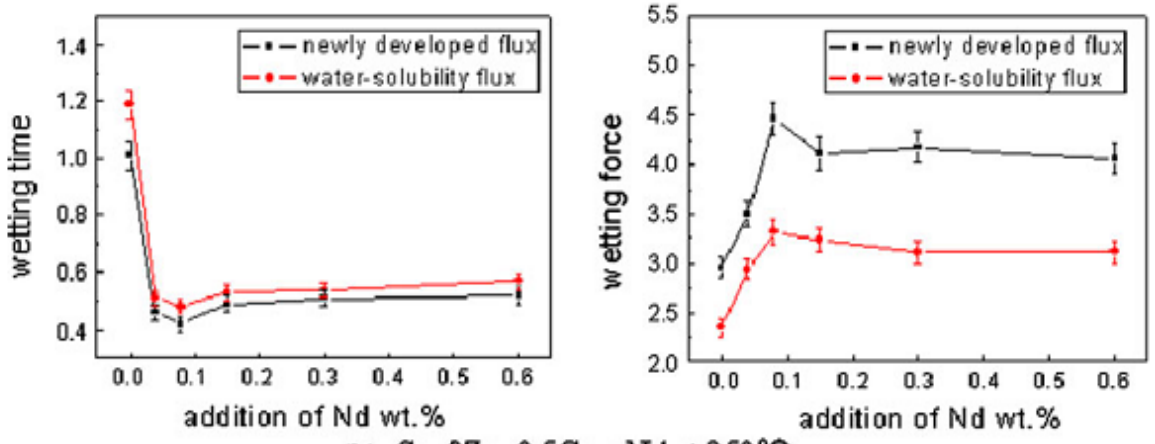
increased with addition of Nd and La [12]. It is found that Sn-Zn solder alloy doped with Ga having better oxidation resistance but adverse effect on surface tension, the wettability were improved and the maximum value was obtained when the addition of Ga is at 0.5 wt% [13-15]. In this particular paper, we analyze the effect of alloying elements on wettability, mechanical properties, microstructure and intermetallic compounds layer of Sn-Zn solder alloy.

II WETTABILITY

Wettability is considered as one of the important property in the development of solder alloy for electronic applications. The tendency of wettability depends on the degree of surface cleanliness as well as the interfacial tensions of the solid/liquid contact systems [16]. Wettability is the tendency of molten solder to spread over solid substrate which is generally indicated with the parameters of interfacial tension and contact angle, as measured by means of wetting spreading test and wetting balance method [17, 18].



(a) Sn–9Zn–0.5Ga–xNd at 240°C



(b) Sn–9Zn–0.5Ga–xNd at 250°C

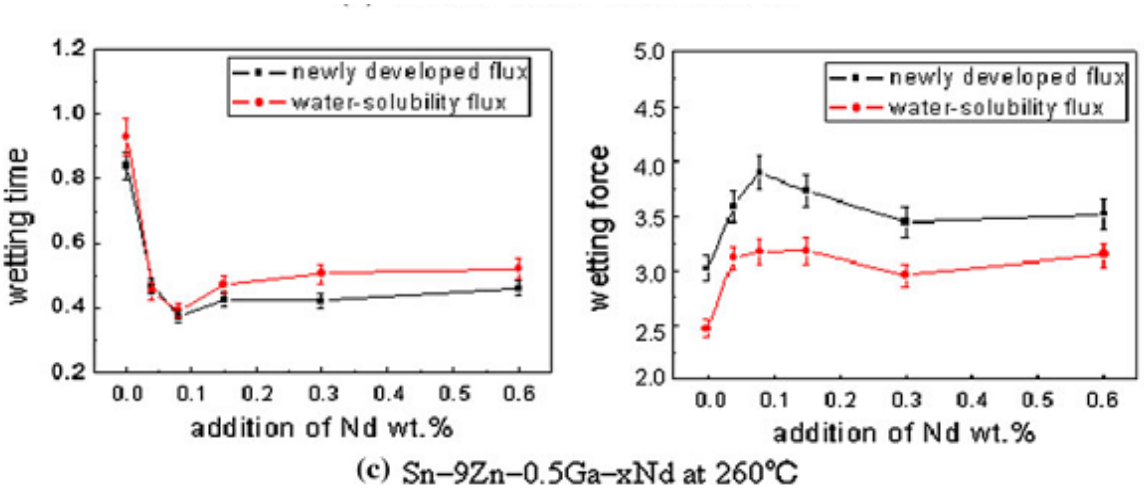


Fig. 1 Wetting properties of Sn-9Zn-0.5Ga lead free solders alloy with addition of Nd

After comparing all the results maximum wettability were obtained at 0.08wt% of Nd. The effect of fluxes and temperatures on wettability shown in fig. 1. It is also obvious that better wettability was obtained with newly developed flux in comparison to water solubility flux [19]. As the temperature increases the wettability further increased. From fig 1b, c it can be found that the wetting forces changes slightly from 240 to 260^{0}C but the wetting times reduced considerably from 240 to 260^{0}C.

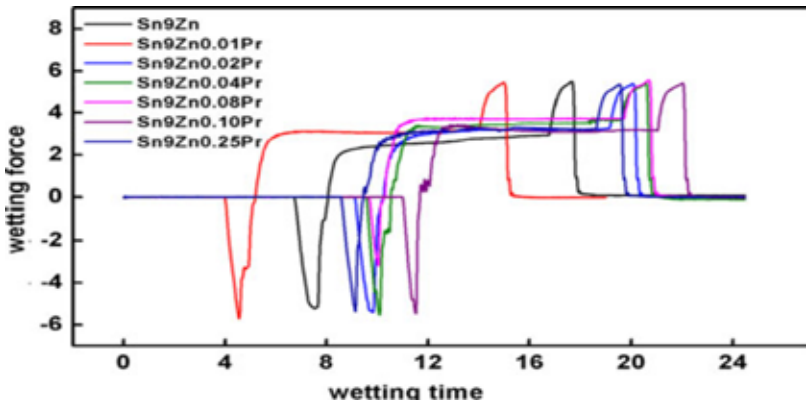


Fig. 2 Wetting curves of Sn-Zn-XPr solder with ZnCl2-NH4Cl flux

It was found that the wetting properties of solder joints improve with Pr addition, and achieve the optimum wettability when the Pr content is 0.08wt%. It's wetting force increases 56% and it's wetting time decreases 40% [20]. The wetting force and wetting time exhibits disproportional characteristics. But when the Pr content up to 0.1wt% does adverse effect on its wettability. Pr is a surface active element with ability to accumulate at the solder interface in the molten state and due to this it not only decreases the surface tension but also reduced the ability of Zn to react with oxygen, which is beneficial to the solder ability of the solder [21]. Fig. 2 shows the original wetting curves for Sn-Zn-XPr solder with $ZnCl_2$-NH_4Cl flux.

III MECHANICAL PROPERTIES

Mechanical properties play a significant role in the metallurgical bond for Sn-Zn based solder alloy. [19] It was found that both shear force and pull force were significantly improved with the addition of Nd upto 0.08wt%.

But with further increase of Nd both shear force and pull force decrease but still higher than the original solder as shown in fig. 3

It was investigated that the shear force of the solder joints gradually increased with the increase of Pr content, and reach the maximum value when Pr content is 0.04wt.%, but with the further increase of Pr upto 0.08wt% the value of shear force little decrease. The similar trend was shown by pull force. When the Pr content is at about 0.08wt.%, the pull force of solder joint reached to the peak value and then decreased with the further increased of Pr. The refined microstructure and bulk Sn-Pr phase formed in the solder are considered as the most important factor to this [21]. The maximum engineering stress a material can withstand in tension along the engineering stress–strain curve is the UTS of the material [22]. It was investigated that the tensile strength of the Sn-9Zn solder increased upto a certain amount of nano Sb content and then decreased similarly the elongation during failure decreased with increasing nano Sb content as listed in table 1. The reason for decrease in mechanical properties with further increase in nano Sb content was the rod shaped IMCs observed in the microstructure of Sn–9Zn/1.5Sb is uniformly distributed in the solder matrix and the Zn-rich phase becomes finer and round with 1.5% nano Sb addition. The second phase IMCs increases the tensile strength up to certain extent and after the threshold percentage value the precipitate start to grow non-coherently resulting in the decrease of overall strength [23].

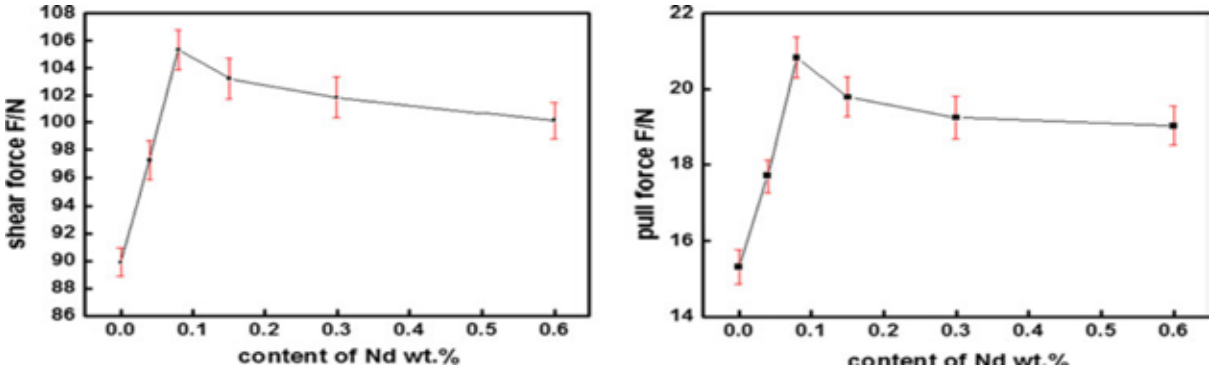


Fig. 3 Mechanical properties of Sn-9Zn-0.5Ga lead free solders joints with addition of Nd

Fig. 4 shows the mechanical properties of Sn-Zn solder alloy depending on the nano Sb content.

The proof strength of the solder alloy increased with increase in nano Sb content and the maximum value of proof strength 44% was observed in Sn-9Zn/1.5Sb alloy.

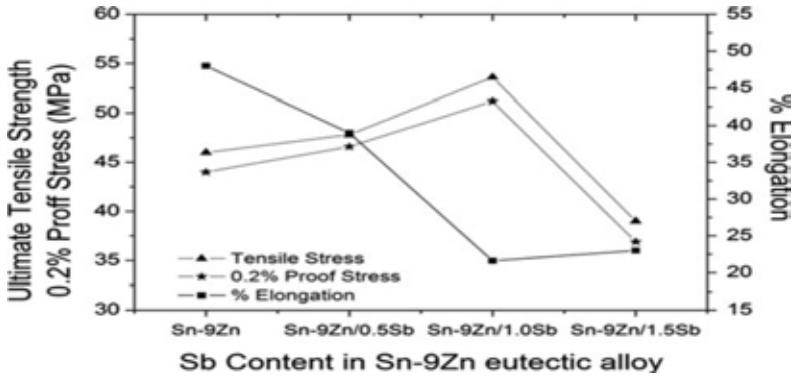


Fig. 5 Tensile properties of Sn–9Zn, Sn–9Zn/0.5Sb, Sn–9Zn/1.0Sb and Sn–9Zn/1.5Sb

Table 1 Mechanical properties of solder alloy

Alloy	Tensile strength(MPa)	Elongation (%)
Sn-9Zn	46	48
Sn-9Zn/0.5Sb	47.8	39
Sn-9Zn/1Sb	53.6	21.6
Sn-9Zn/1.5Sb	39	23

IV MICROSTRUCTURES

Rare earth elements are the highly surface active elements which play vital role in metallurgical issue of materials, such as microstructure refinement, inhabitation of the excessive intermetallic growth in solder interface [2, 24]. The results indicate that the solid solubility of Sn in Zn ranges from 0.05 wt% to 2 wt% [25]. But with the addition of nano Sb particles e-Sb_3Zn_4 IMC were clearly identified as well as the acicular shaped α-Zn turns in to fine α-Zn phases in the β-Sn matrix as shown in fig. 5. It was found that with an increase of nano Sb content α-Zn phase get finer [23]. On the other hand, the conversion of acicular Zn rich phase in to fine phase due to the fact that the nano Sb particles act as sites of heterogeneous nucleation for Zn rich phase as shown in fig. 6.

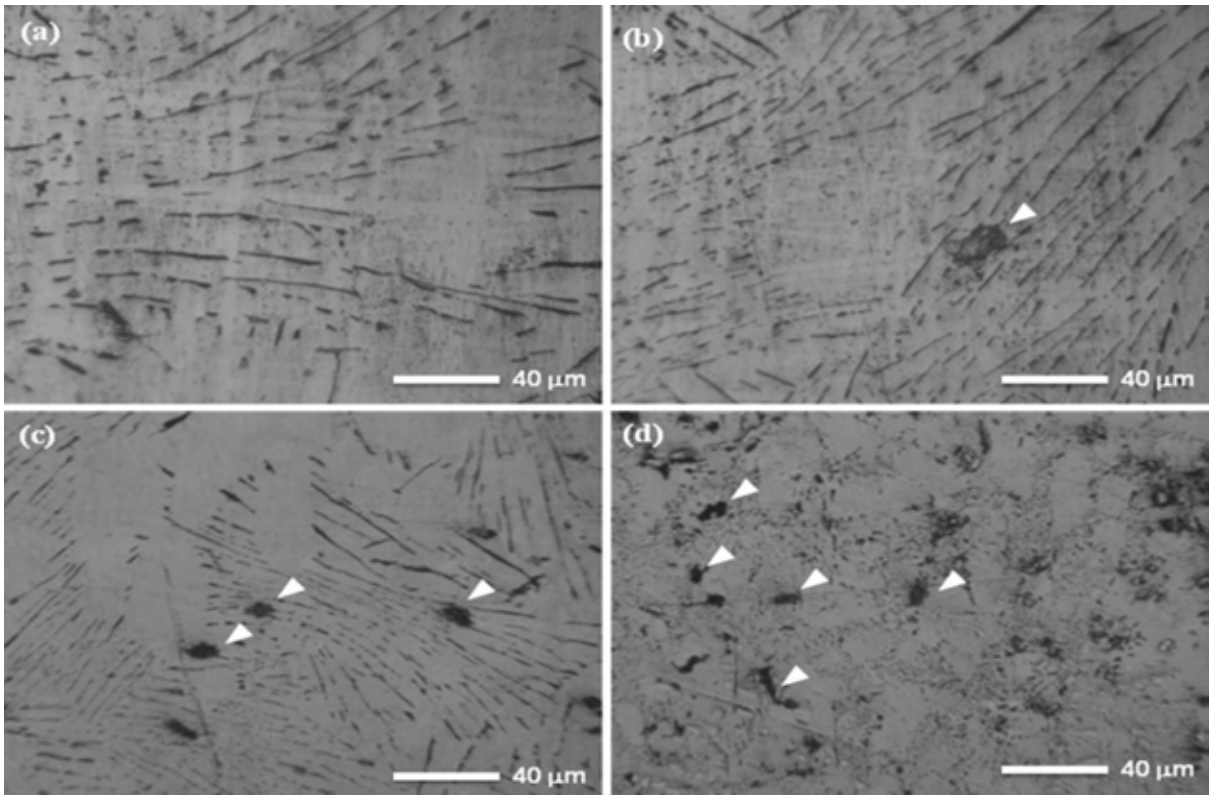


Fig. 6 Optical micrographs of chill-cast samples of a Sn–9Zn, b Sn–9Zn/0.5Sb, c Sn–9Zn/1.0Sb, and d Sn–9Zn/1.5Sb alloys (all images taken at 400X)

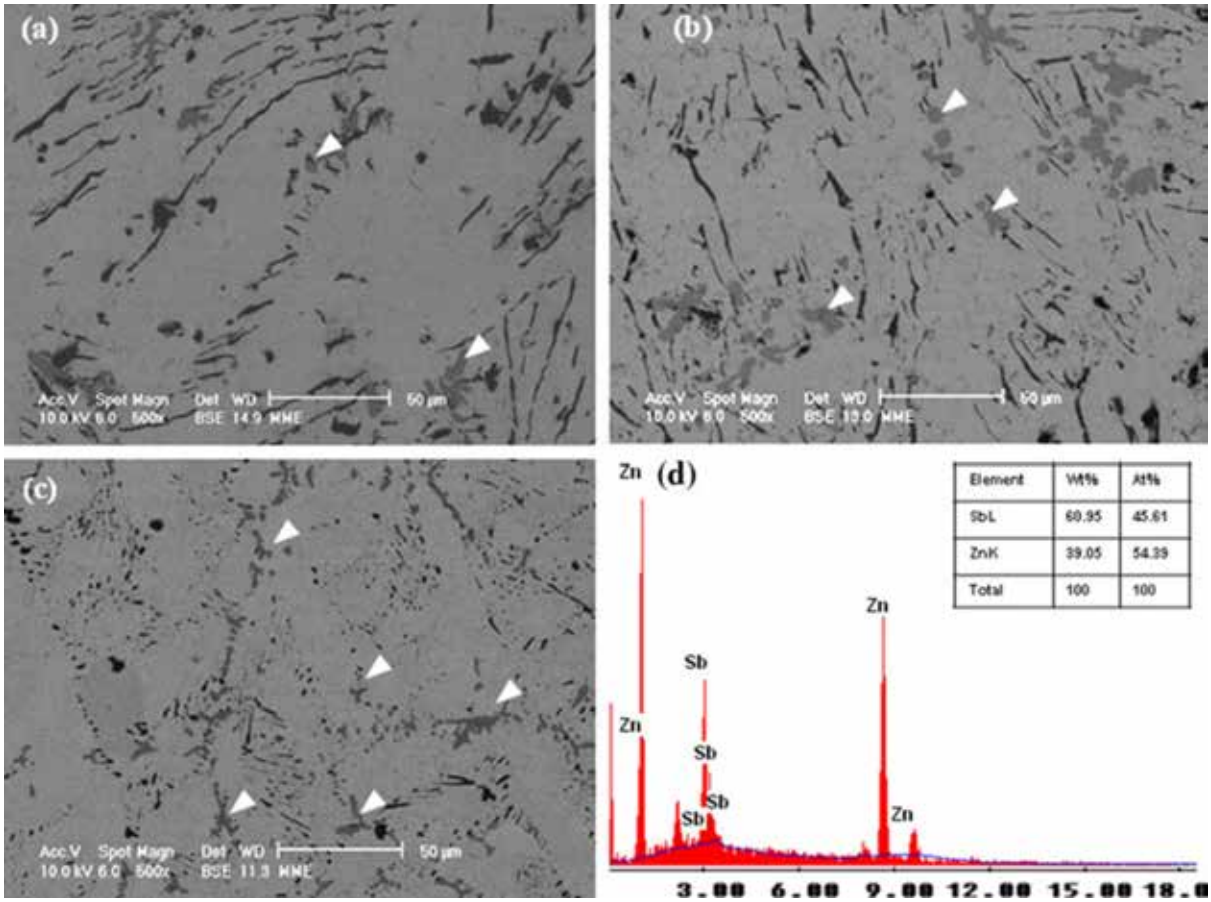


Fig. 7 SEM micrographs of chill-cast samples of a Sn–9Zn/ 0.5Sb, b Sn–9Zn/1Sb, c Sn–9Zn/1.5Sb, alloys and d EDS profiles

Due to addition of Ga to Sn-9Zn solder, the Zn rich phase became smaller. With the addition of Nd into the Sn-9Zn-0.5Ga solder the zinc rich phase further decreased and turns into pot like. According to the grain-refining strengthening theory, the refined microstructure will have a favourable effect on the mechanical properties; the strength of the alloy will increase significantly after adding Nd. It was investigated that when Nd added less then 0.15wt% has favourable effect on grain refinement. But when the Nd increased to 0.15 wt% some dark particulate-shaped phases appeared and these dark phases are $NdSn_3$ compounds. With the further addition of Nd the dark phases also increased. Since these Sn–Nd IMCs possess high melting temperature, the formation of Sn–Nd phase played a role as the heterogeneous sites for nucleation, resulted in the opposite effects on the properties of the solders [19]. The EDS analysis revealed that they were composed of Sn and Zn and having approximately 3:1 atomic ratio. It was investigated that with the addition of 0.01–0.08% Pr to the Sn-9Zn alloy, the volume fraction and size of the needle like phase tends to be decreased, and obtain finest and uniform structure when 0.08 wt% Pr is added, as show in Fig. 7b–d. When Pr content is up to 0.1%, some dark particulate-shaped phases, about 3–6 um, can be observed in the Sn-rich matrix. These dark phases are determined as the Sn-Pr intermetallic compounds by EDS analysis. The atomic ratio between Sn and Pr is approximately 3:1. According to the Sn-Pr phase diagram we can infer that the black phase probably is the PrSn3 compound.

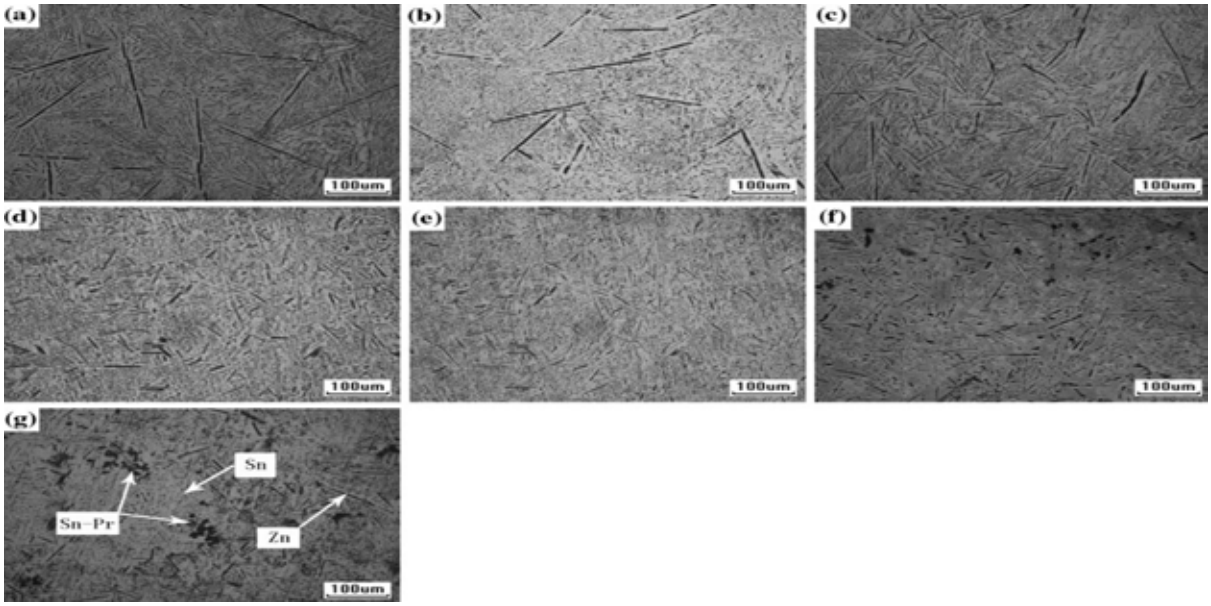


Fig.8 Optical micrographs of a Sn-9Zn, b Sn-9Zn-0.01%Pr, c Sn-9Zn-0.02%Pr, d Sn-9Zn-0.04Pr, e Sn-9Zn-0.08%Pr, f Sn-9Zn 0.1%Pr and g Sn-9Zn-0.25Pr

With further increase of Pr content, both the size and volume fraction of the dark phases further increase, as show in Fig. 8g. The rare earth Pr react with Sn to form Sn-Pr intermetallics, which can reduce the driving force for the formation of primary IMC in solidification process. In addition, the primary Sn-Pr phase take the form of insoluble, solid particles since its high melting temperature, which can play a role as the heterogeneous sites for nucleation. But with the increase of Pr content, large amount of Sn-Pr compounds formed, and part of them will gather together and grow up, and finally bulk Sn-Pr compounds was observed in the Sn-9Zn-0.25Pr solder, which does the opposite effect on the properties of the solder [21].

V INTERMETALLICS

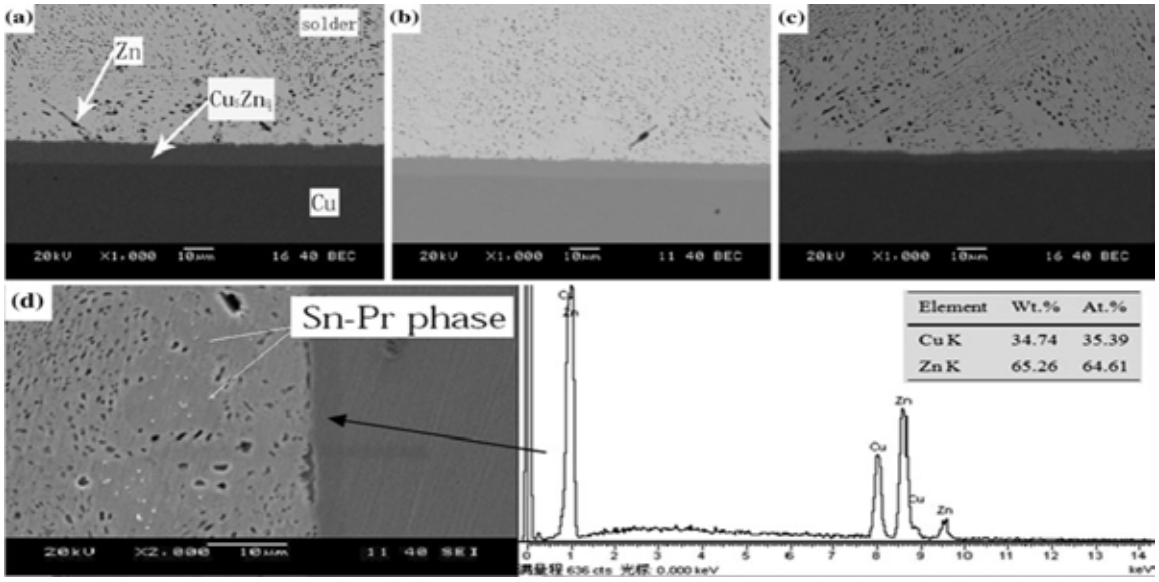


Fig. 8 The interface microstructure of solder/Cu a Sn-9Zn/Cu, b Sn-9Zn-0.02Pr/Cu, c Sn-9Zn-0.08Pr/Cu, d Sn-9Zn-0.25Pr/Cu

During soldering, the solder alloy spreads over metallic electrodes to form particular reaction products at interfaces or inside the solder [26]. Such IMC formation sometimes effects the structural integrity of interfaces. Due to reaction between soldered joints and substrate, it is desirable to achieve a good metallurgical bond, however, excessive IMC growth may have a negative effect on the reliability of soldered joints [27]. Therefore, the reaction between the molten, or solid solder, and a metallic substrate is very important because it plays a major role in determining the microstructure and strength of the soldered joints.

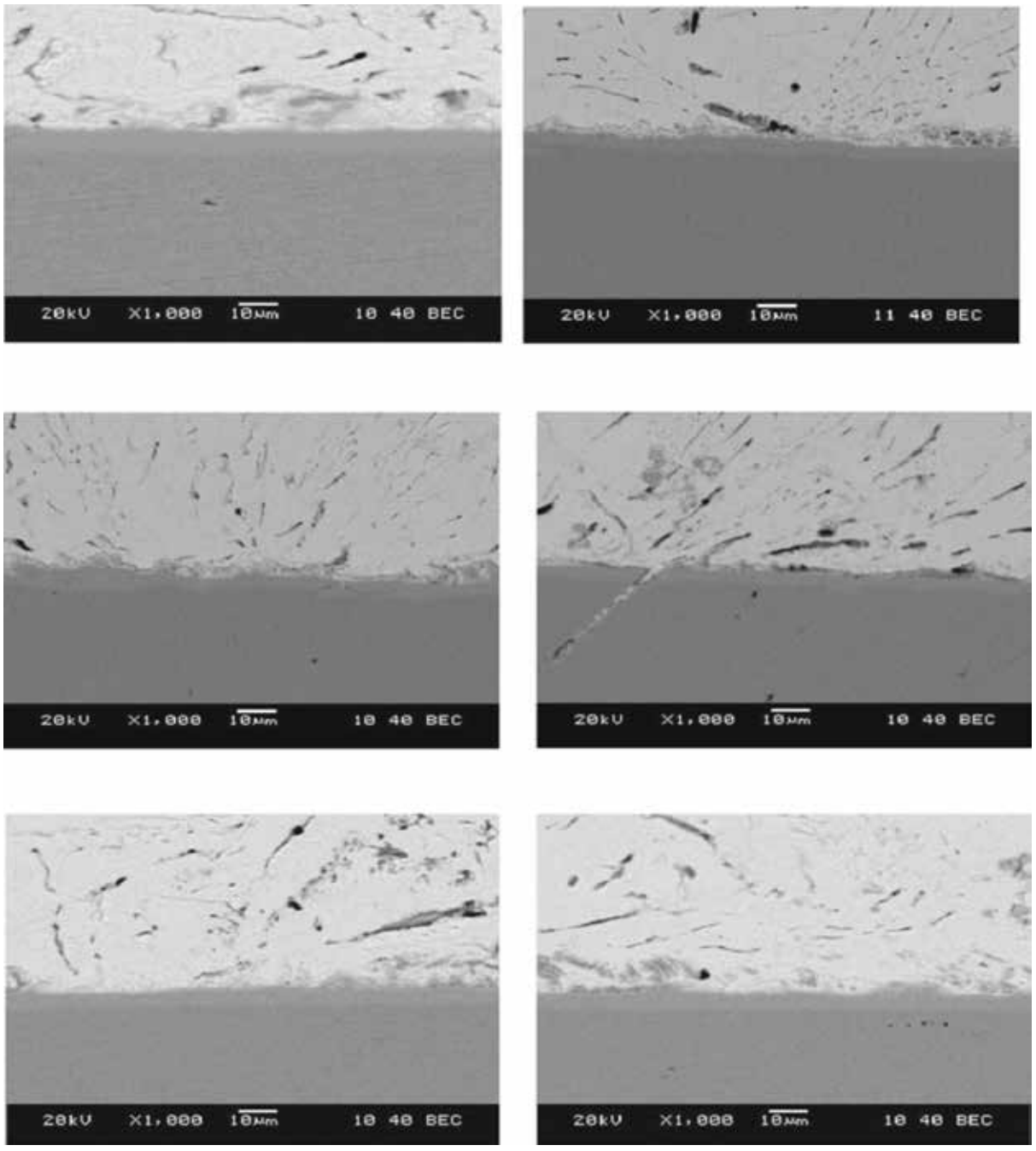


Fig. 9 Effect of Nd addition on the growth of the IMC at Sn–Zn Ga/Cu interface

It was found that with the addition of Pr the growth of intermetallic was depressed as shown in fig. 8. The reason for depress the growth of IMC layer may be summarized as follows: due to the reaction between Cu and

Zn makes a tin-rich area was formed near the IMC layer, part of the PrSn3 particles formed in as-cast solder may remelting during soldering, due to the large difference between electro negativity between Sn and Pr, the remelted Pr will diffuse to the tin-rich area and reform $PrSn_3$ particles, which will act as the diffusion barrier of copper and zinc, thus depress the growth of the IMC layer. At the same time, this also explain why bulk PrSn3 particles was observed in the vicinity of IMC layer with 0.25wt.% Pr addition, as show in Fig. 8d. In addition, the reformed stable $PrSn_3$ intermetallic particles in molten solder play a role as the heterogeneous nucleation sites and promote the solidification process. Thus, the reaction time of liquid solder with the Cu substrate is dec--reased during soldering, and a lower intermetallic thickness is obtained [21].

It was observed that a small amount of Nd addition can decreased the growth of the IMC at Sn–Zn Ga/Cu interface as shown in fig. 9, the intermetallic thickness of Sn–9Zn–0.5Ga–0.08Nd/Cu decreased by approximately 20% compared with the Sn–Zn–0.5Ga solder [19]. It was also found that with the increase of Nd, Sn–Nd phase can be observed at the solder/Cu interface and a mass of NdSn3 formed which was assumed to be unfavourable to the mechanical properties of soldered joints [28].

VI CONCLUSION

The addition of trace amounts of rare earth elements enhance the properties and reliability of lead free solder alloys making the resulting alloy better alternative for Sn-Pb solder.

1. The wettability of the Sn-9Zn solder was enhanced with 0.08wt. % Pr addition because the surface tension of molten solder is decreased on the hand the wettability of Sn–9Zn–0.5Ga solder was improved with the addition of rare earth Nd and the best point of wettability achived when the addition of Nd is at 0.08 wt%.
2. The mechanical properties of solder joint increased with the addition of RE elements have been greatly improved because rare earths can refine microstructure and bulk phase are regarded as the most important factors.
3. With the trace amount of RE the volume fraction and the size of needle-like rich Zn phase in the Sn-9Zn solder trends to be decreased, and obtain finer and uniform structure.
4. The thickness of the interfacial layer of Sn-9Zn/Cu substrate is remarkably depressed with RE elements addition.

REFERENCES

[1] J.O. Kim, J.P. Jung, J.H. Lee, J. Suh, H.S. Kang, Effects of laser parameters on the characteristics of a Sn-3.5 wt. % Ag solder joint. *Met. Mater. Int. 15(1),* 119–123 (2009)

[2] L. Zhang, S.B. Xue, Y. Chen, Z.J. Han, J.X. Wang, S.L. Yu, F.Y. Lu, Effects of cerium on Sn-Ag-Cu alloys based on finite element simulation and experiments. *J. Rare Earths 27(1),* 138– 144 (2009)

[3] J.B. Pan, B.J. Toleno, T.C. Chou, W.J. Dee, The effect of reflow profile on SnPb and SnAgCu solder joint shear strength. *Solder. Surf. Mt. Technol. 18(4),* 48–56 (2006)

[4] Y.L. Gao, C.D. Zou, B. Yang, Q.J. Zhai, J. Liu, E. Zhuravlev, C. Schick, Nanoparticles of SnAgCu lead-free solder alloy with an equivalent melting temperature of SnPb solder alloy. *J. Alloy. Compd. doi:10.1016/j.jallcom.2009.05.042*

[5] L.H. Qi, J.H. Huang, J.G. Zhang, Y. Wang, Growth behavior of intermetallic compounds on Sn-3.5Ag-0.5Cu/Cu(Ni) interface under thermal-shearing cycling condition. *Rare Met. Mater. Eng. 36(2),* 241–244 (2007)

[6] S.B. Xue, Y. Chen, X.C. Lv, Y.P. Liao, Effect of cerium on wettability and mechanical properties of soldered joints for Sn Ag Cu lead free solder. *Trans. China Weld. Inst. 26(10),* 1–4 (2005)

[7] S.B. Xue, L. Zhang, L.L. Gao, S.L. Yu, H. Zhu, Current Situation and Prospect on Lead-free Solders affected with micro alloying elements. *Weld. Join. 3(3),* 24–33 (2009)

[8] K.L. Lin, C.L. Shih, Microstructure and thermal behavior of Sn-Zn-Ag solders. *J. Elec. Materi. 32(12),* 1496–1500 (2003)

[9] X. Chen, A.M. Hu, M. Li, D.L. Mao, Study on the properties of Sn-9Zn-xCr lead-free solder. *J. Alloys Compd.* 460, 478–484 (2008)

[10] H. Wang, S.B. Xue, Z.J. Han, J.X. Wang, Research status and prospect of Sn-Zn based lead-free solders. *Weld. Join. (2),* 31–35 (2007)

[11] S. Wu, H. Kang, P. Qu, Study of Sn-Zn lead-free solder by alloying. *Electron. Process Technol. 29(2),* 66–70 (2008)

[12] J. Zhou, Y.S. Sun, F. Xue, Effect of Nd and La on surface tension and wettability of Sn-8Zn-3Bi. *Trans. Nonferr. Met. Soc. China 15(5),* 1161–1165 (2005)

[13] H. Wang, Study on the properties and related mechanisms of micro-alloyed Sn–9Zn lead-free solder.[D], *Nanjing: Nanjing University of Aeronautics and Astronautics,* 2010

[14] N.S. Liu, K.L. Lin, The effect of Ga content on the wetting reaction and interfacial morphology formed between Sn–8.55Zn– 0.5Ag–0.1Al–xGa solders and Cu. *Scripta Mater. 54(2),* 219–224 (2006)

[15] W.X. Chen, S.B. Xue, H. Wang, Wetting properties and interfacial microstructures of Sn–Zn–xGa solders on Cu substrate. *Mater. Des. 31*, 2196–2200 (2010)

[16] S.P. Yu, H.J. Lin, M.H. Hon, Effects of process parameters on the soldering behavior of the eutectic Sn-Zn solder on Cu substrate. *J. Mater. Sci. Mater. Electron. 11(6),* 461–471 (2000)

[17] H. Wang, S.B. Xue, W.X. Chen, F. Zhao, J. Mater. Sci.: Mater. Electro. 20(12), 1239–1246 (2009)

[18] C. Kim, S. Kang, D. Baldwin, *J. Appl. Phys. 104(3),* 3537 (2008)

[19] P. Xue, S.b. Xue, Y.f. Shen, H. Zhu, L.l. Gao, Study on properties of Sn–9Zn–Ga solder bearing Nd. *J Mater Sci: Mater Electron* (2012) *23:*1272–1278

[20] L. Wang, D.Q. Yu, J. Zhao, M.L. Huang, Improvement of wettability and tensile property in Sn-Ag-RE lead-free solder alloy. *Mater. Lett. 56(6),* 1039–1042 (2002)

[21] Z. Xiao, S. Xue, Y. Hu, H. Ye, L.Gao, H. Wang, Properties and microstructure of Sn-9Zn lead-free solder alloy bearing Pr. *J Mater Sci: Mater Electron* (2011) *22*:659–665

[22] W.D. Callister, Materials Science and Engineering an Introduction, 4th edn. (Wiley, Canada, 1996)

[23] I. Shafiq, Y. C. Chan, N. B. Wong, W. K. C. Yung, Influence of small Sb nanoparticles additions on the microstructure, hardness and tensile properties of Sn–9Zn binary eutectic solder alloy. *J Mater Sci: Mater Electron* (2012) *23*:1427–1434

[24] L. Zhang, S.B. Xue, L.L. Gao, G. Zeng, Z. Sheng, Y. Chen, S.L. Yu, Effects of rare earths on properties and microstructures of lead-free solder alloys. *J. Mater. Sci. Mater. Electron. 20(8),* 685– 694 (2009)

[25] J. Chang, S.-K. Seo, H.M. Lee, Phase equilibria in the Sn-Ni-Zn ternary system: Isothermal sections at 200^0C, 500^0C, and 800^0C. *J. Electron. Mater. 39(12)*, 2643–2652 (2010)

[26] C.W. Hwang, K.S. Kim, K. Suganuma, Interfaces in lead-free soldering. *J. Elec. Materi. 32(11)*, 1249–1256 (2003)

[27] L. Zhang, S.B. Xue, L.L. Gao, Y. Chen, S.L. Yu, Z. Sheng, G. Zeng, Effects of trace amount addition of rare earth on properties and microstructure of Sn-Ag-Cu alloys. *J. Mater. Sci. Mater. Electron. 20(12)*, 1193–1199 (2009)

[28] Y.H. Hu, S.B. Xue, H. Wang, H. Ye, Effects of rare earth element Nd on the solderability and microstructure of Sn–Zn lead-free solder. *J. Mater. Sci.: Mater. Electron. 22(5)*, 481–487 (2011)

FPGA IMPLEMENTATION OF AES ALGORITHM

S.A. Annadate[1] , Nitin Ram Chavan[2]

[1,2] *Electronics and Telecommunication Dept, J N Collage of engineering Aurangabad, (India)*

ABSTRACT

Advanced Encryption Standard (AES)is an FIPS approved cryptographic algorithm that can be used to protect electronic data. The AES can be programmed in software or built with pure hardware. However FPGA offer a quicker and more customizable solution. This paper presents the AES algorithm with regard to FPGA and the Very High Speed Integrated Circuit Hardware Description language (VHDL). ModelSim SE PLUS 5.7g software is used for simulation and optimization of the synthesizable VHDL code. Synthesizing and implementation (i.e. Translate, Map and Place and Route) of the code is carried out on Xilinx - Project Navigator, ISE 8.2i suite. All the transformations of both Encryption and Decryption are simulated using an iterative design approach in order to minimize the hardware consumption. Xilinx XC3S400 device of Spartan Family is used for hardware evaluation. This paper proposes a method to integrate the AES encrypter and the AES decrypter. This method can make it a very low-complexity architecture, especially in saving the hardware resource in implementing the AES (Inv) Sub Bytes module and (Inv) Mix columns module etc Besides, the architecture can still deliver a high data rate that suited for hardware-critical applications, such as smart card, PDA, and mobile phone etc.

Keywords: AES, Encryption Decryption, FPGA, VHDL, Xilinx.

I INTRODUCTION

1.1 General

Cryptography, often called encryption, is the practice of creating and using a cryptosystem or cipher to prevent all but the intended recipient(s) from reading or using the information or application encrypted. A cryptosystem is a technique used to encode a message. The recipient can view the encrypted message only by decoding it with the correct algorithm and keys. Cryptography is used primarily for communicating sensitive material across computer networks[3]. The process of encryption takes a clear-text document and applies a key and a mathematical algorithm to it, converting it into crypto-text. In crypto-text, the document is unreadable unless the reader possesses the key that can undo the encryption. In 1997 the National Institute of Standards and Technology (NIST), a branch of the US government, started a process to identify a replacement for the Data Encryption Standard (DES). It was generally recognized that DES was not secure because of advances in computer processing power. The goal of NIST was to define a replacement for DES that could be used for non-military information security applications by US government agencies. Of course, it was recognized that commercial and other non-government users would benefit from the work of NIST and that the work would be generally adopted as a commercial standard. The NIST invited cryptography and data security specialists from

around the world to participate in the discussion and selection process. Five encryption algorithms were adopted for study. Through a process of consensus the encryption algorithm proposed by the Belgium cryptographers Joan Daeman and Vincent Rijmen was selected. Prior to selection Daeman and Rijmen used the name Rijndael (derived from their names) for the algorithm[3]. After adoption the encryption algorithm was given the name Advanced Encryption Standard (AES) which is in common use today. In 2000 the NIST formally adopted the AES encryption algorithm and published it as a federal standard under the designation FIPS-197. The full FIPS-197 standard is available on the NIST web site (see the Resources section below). As expected, many providers of encryption software and hardware have incorporated AES encryption into their products[1].

The AES encryption algorithm is a block cipher that uses an encryption key and a several rounds of encryption. A block cipher is an encryption algorithm that works on a single block of data at a time. In the case of standard AES encryption the block is 128 bits, or 16 bytes, in length. The term “rounds” refers to the way in which the encryption algorithm mixes the data re-encrypting it ten to fourteen times depending on the length of the key. This is described in the Wikipedia article on AES encryption. The AES algorithm itself is not a computer program or computer source code. It is a mathematical description of a process of obscuring data. A number of people have created source code implementations of AES encryption, including the original authors[6].

AES encryption uses a single key as a part of the encryption process. The key can be 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length. The term 128-bit encryption refers to the use of a 128-bit encryption key. With AES both the encryption and the decryption are performed using the same key. This is called a symmetric encryption algorithm. Encryption algorithms that use two different keys, a public and a private key, are called asymmetric encryption algorithms. An encryption key is simply a binary string of data used in the encryption process. Because the same encryption key is used to encrypt and decrypt data, it is important to keep the encryption key a secret and to use keys that are hard to guess. Some keys are generated by software used for this specific task. Another method is to derive a key from a pass phrase. Good encryption systems never use a pass phrase alone as an encryption key.NIST was aware of side channel attacks when evaluating all the finalists[2]. Comparing the Rijndael algorithm security against side channel attacks to the other four finalists considered by NIST they concluded:

- Rijndael and Serpent use only Boolean operations, table lookups, and fixed Shifts/rotations. These operations are the easiest to defend against attacks.
- Two fish uses addition, which is somewhat more difficult to defend against Attacks.
- MARS and RC6 use multiplication/division/squaring and/or variable Shift/rotation. These operations are the most difficult to defend.

1.2 Objective

This paper presents the AES algorithm with regard to FPGA and the Very High Speed Integrated Circuit Hardware Description language (VHDL). ModelSim SE PLUS 5.7g software is used for simulation and optimization of the synthesizable VHDL code. Synthesizing and implementation (i.e. Translate, Map and Place and Route) of the code is carried out on Xilinx - Project Navigator, ISE 8.2i suite.

1.3 Existing system

Data Encryption Standard (**DES**) is a block cipher (a form of shared secret encryption) that was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed wide**s**pread use internationally. It is based on a symmetric-key algorithmthat uses a 56-bit key. The algorithm was initially controversial with classified de**s**ign elements, a relatively short key length, and suspicions about a National Security Agency (NSA) backdoor. DES consequently came under intense academic scrutiny, which motivated the modern understanding of block ciphers and their cryptanalysis.

Data Encryption Standardpreviously pre-dominant algorithm for the encryption. It was highly influential in the advancement of modern cryptography in the academic world. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small.There are also some analytical results which demonstrate theoretical weaknesses in the cipher. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES). Furthermore, DES has been withdrawn as a standard by the National Institute of Standards and Technology.

Encryption algorithm play an important role in communication security where encryption time, Memory usages output byte and battery power are the major issue of concern. The selected encryption AES, DES algorithms are used for performance evaluation. Based on the text files used and the experimental result it was concluded that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm and DES Algorithm.

1.4 Proposed system

In this proposed System presents various software implementations of the AES algorithm with different data and task parallelism granularity, and shows that AES implementations on a fine grained many-core system can achieve high performance, throughput per unit of chip area and energy efficiency compared to other software platforms. Maximum speed and lesser area by mapping all the four Logical functions of AES to LUTs, ROMs and Block RAMs. The proposed architecture has three parts

1. Key Generation Module
2. Encryption Module
3. Decryption Module.

II HARDWARE IMEMENTATION OF AES

2.1 General

A many-core processor is a single computing component with two or more independent actual central processing units (called "cores"), which are the units that read and execute program instructions. The instructions are ordinary CPU instructions such as add, move data, and branch, but the multiple cores can run multiple instructions at the same time, increasing overall speed for programs amenable to parallel computing. Manufacturers typically integrate the cores onto a single integrated circuit die (known as a chip multiprocessor or CMP), or onto multiple dies in a single chip package.

Many-core processors are widely used across many application domains including general-purpose, embedded, network, digital signal processing (DSP), and graphics. The improvement in performance gained by the use of a multi-core processor depends very much on the software algorithms used and their implementation. In particular, possible gains are limited by the fraction of the software that can be run in parallel simultaneously on multiple cores; this effect is described by Amdahl's law. In the best case, so-called embarrassingly parallel problems may realize speedup factors near the number of cores, or even more if the problem is split up enough to fit within each core's cache(s), avoiding use of much slower main system memory. Most applications, however, are not accelerated so much unless programmers invest a prohibitive amount of effort in re-factoring the whole problem. The parallelization of software is a significant ongoing topic of research.

The terms multi-core and dual-core most commonly refer to some sort of central processing unit (CPU), but are sometimes also applied to digital signal processors (DSP) and system-on-a-chip (SoC). The terms are generally used only to refer to multi-core microprocessors that are manufactured on the same integrated circuit die; separate microprocessor dies in the same package are generally referred to by another name, such as multi-chip module. This article uses the terms "multi-core" and "dual-core" for CPUs manufactured on the same integrated circuit, unless otherwise noted.

2.2 AES algorithm modules

Key board,FPGA,LCD

2.3 Module description of FPGA

Sub bytes : The Sub Bytes operation is a nonlinear byte substitution. Each byte from the input state is replaced by another byte according to the substitution box (called the S-box). The S-box is computed based on a multiplicative inverse in the finite field GF (2^8) and a bitwise affine transformation.

In this module The implementation of the composite field S-BOX is accomplished using combinational logic circuits rather than using pre-stored S-BOX values. S-BOX substitution starts by finding the multiplicative inverse of the number in [7]

Fig 1.Internal bocks

Addition in GF (2^4): Addition of 2 elements in Galois Field can be translated to simple bitwise XOR operation Addition of 2 elements in Galois Field can be translated to simple bitwise XOR operation.

GF (2^4) multiplier: Sub Bytes is a nonlinear transformation that uses 16 byte substitution tables (S-Boxes). An S-Box is the multiplicative inverse of a Galois field GF (2^4) followed by an affine transformation.

Although two Galois Fields of the same order are isomorphic, the complexity of the field operations may heavily depend on the representations of the field elements. Composite field arithmetic can be employed to reduce the hardware complexity. Three multipliers in GF (2^4) are required as a part of finding the multiplicative inverse in GF (2^8). Fig. shows the GF (2^4) multiplier circuit. As can be seen from the figure the GF (2^4) multipliers consist of 3 GF (2^2) multipliers with 4 XOR Gates and with constant multiplier θ. This constant multiplier which has 2 bits input extracts the lower bit output as the higher bit input, while the higher output bit will be the result of XOR operation between the 2 input bits. Full derivation of this multiplier circuit can be found[7].

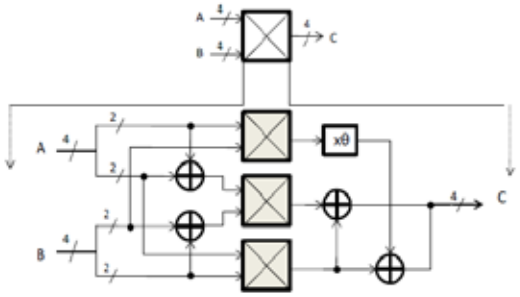


Fig 2. GF (2^4) Multiplier

GF (2^2) Multiplier: While each finite field is itself not infinite, there are infinitely many different finite fields; their number of elements (which is also called cardinality) is necessarily of the form p^n where p is a prime number and n is a positive integer.

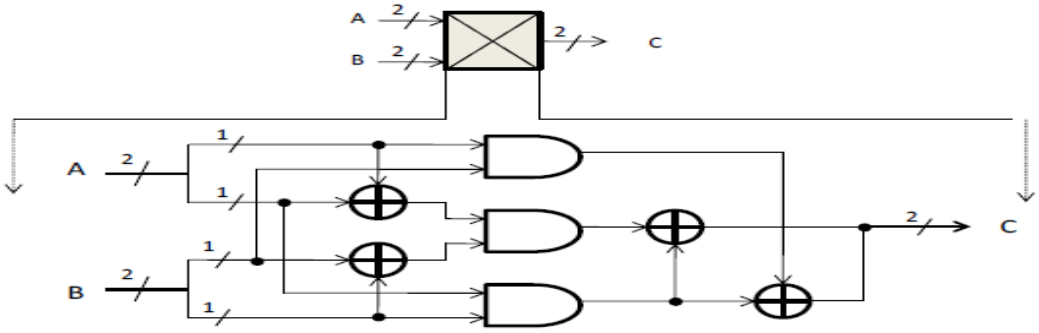


Fig 3.Implimentation of the GF (2^2) multiplier

GF (2^4) squarer: It consists of bitwise xor operation. A bitwise operation operates on one or more bit atterns or binary numerals at the level of their individual bits. It is a fast, primitive action directly supported by the processor, and is used to manipulate values for comparisons and calculations. On simple low-cost processors, typically, bitwise operations are substantially faster than division, several times faster than multiplication, and sometimes significantly faster than addition. While modern high-performance processors usually perform addition and multiplication as fast as bitwise operations, the latter may still be optimal for overall power/performance due to lower resource use.

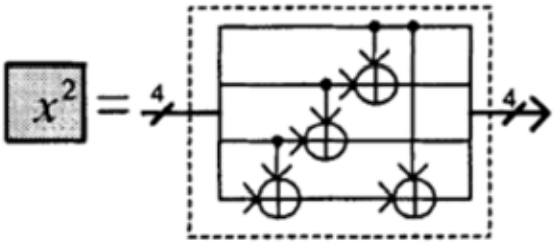


Fig 4.Hardware diagram for Squarer in GF (2^4)

Constant multiplier (Xϕ):

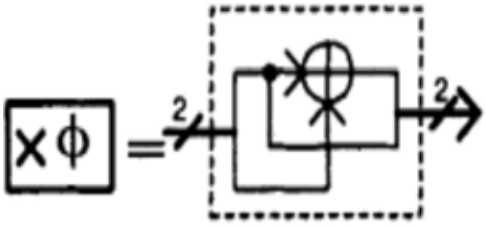


Fig 5.Hardware implementation of multiplication with constant Φ

Constant multiplier (L):

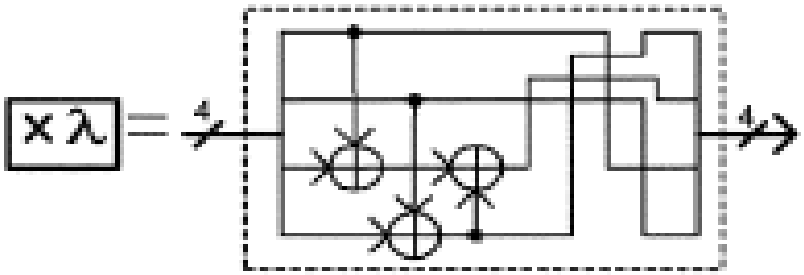


Fig 6.Hardware diagram for multiplication with constant

S-box:

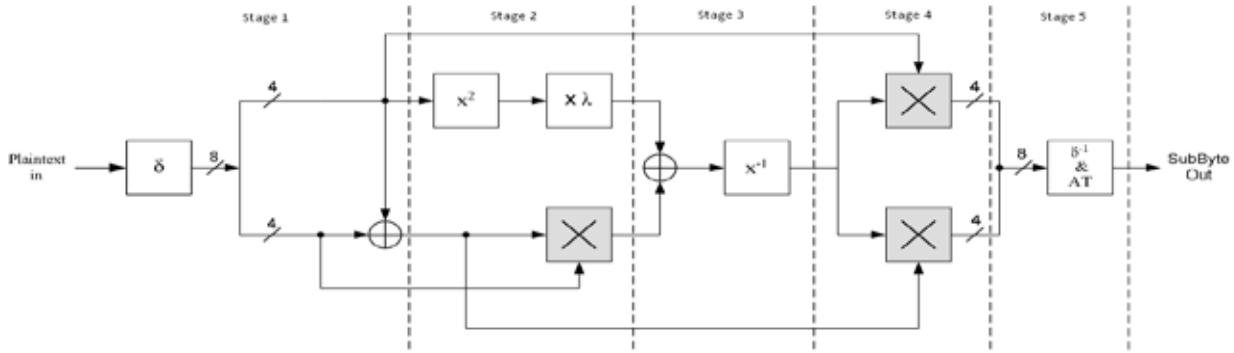
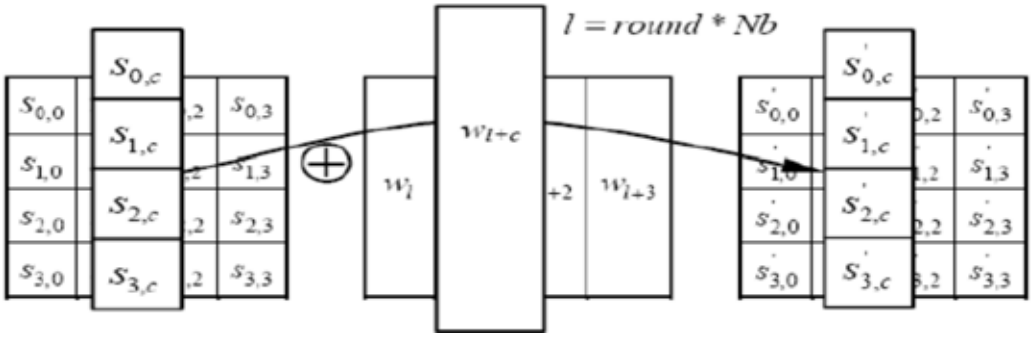


Fig 7. Implemented hardware architecture on the FPGA

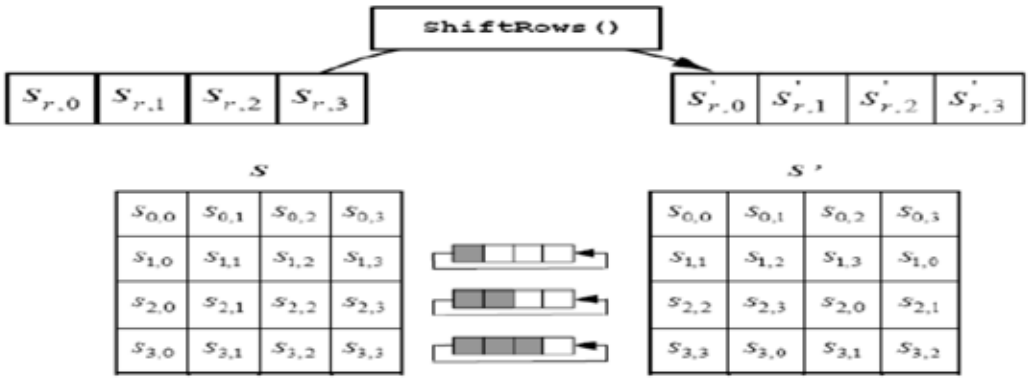
AddRoundKeyTransformation:

In the Add Round Key transformation, a round key is added to the state by Bitwise Exclusive-OR (XOR) operation. Figure below illustrates the Add Round Key. This transformation is the same for both encryption and decryption.



Shift Rows Transformation (Inv Shift Rows):

Shift Rows is a cyclic shift operation in each row of the State. In this operation, the bytes in the first row of the state do not change. The second, third, and fourth rows shift cyclically to the left one byte, two bytes, three bytes, respectively, as illustrated in Figure. The reverse process, inv Shift Row, operates in reverse order to Shift Rows.



Mix Column Transformation (Inv Mix Column):

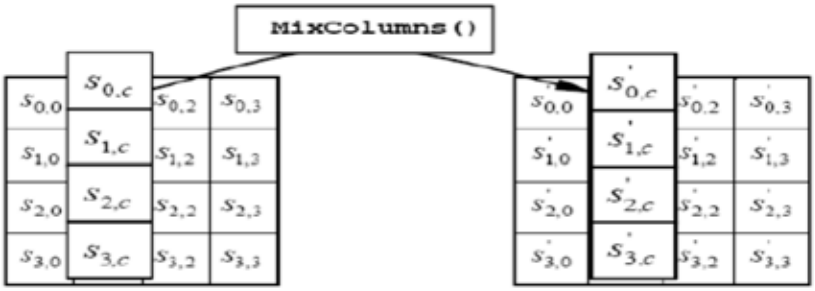
The Mix Column transformation is performed independently on the state Column-by-column. Each column is considered as four term polynomial over GF (2^8) and multiplied by

$a(x)$ modulo $(x4 + 1)$ where $a(x) = \{03\}x3 + \{01\}x2 + \{01\}x + \{02\}$

This transformation can be expressed in matrix form as

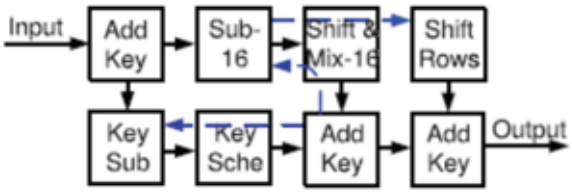
$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} \{02\} & \{03\} & \{01\} & \{01\} \\ \{01\} & \{02\} & \{03\} & \{01\} \\ \{01\} & \{01\} & \{02\} & \{03\} \\ \{03\} & \{01\} & \{01\} & \{02\} \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

For *invMixColumn()*, replace $a(x) = \{0E\}x^3 + \{09\}x^2 + \{0D\}x + \{0B\}$.



Small Encryption:

The Small model implements an AES cipher on FPGA with the fewest processing Elements. As shown in bellow Fig, it requires at least eight blocks to implement an AES cipher with online key expansion process, since each Block on FPGA has only a 128 X 32-bit instruction memory and a 128 X 16-bit data memory[5].



III SIMULATION AND RESULTS

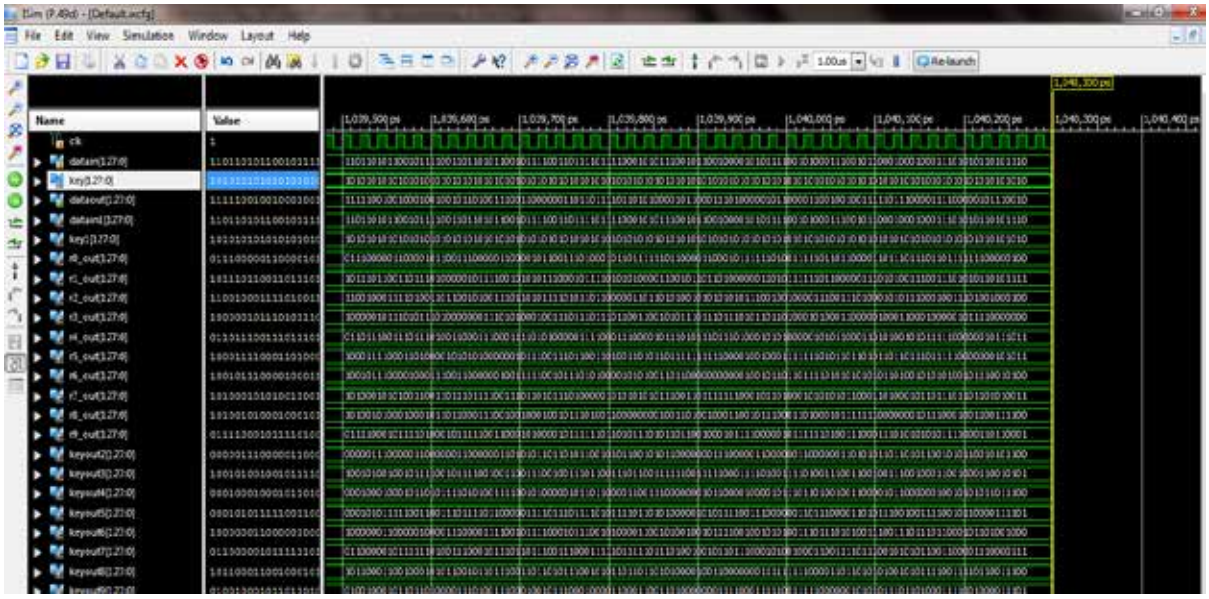
VHDL is used as the hardware description language because of the flexibility to exchange among environments. The software used for this work is Xilinx ISE and the waveforms are simulated with the help of model sim

simulator. This is used for writing, debugging, simulating and checking the performance results using the simulation tools available on Xilinx ISE. The delay is calculated with three different Device families [7].

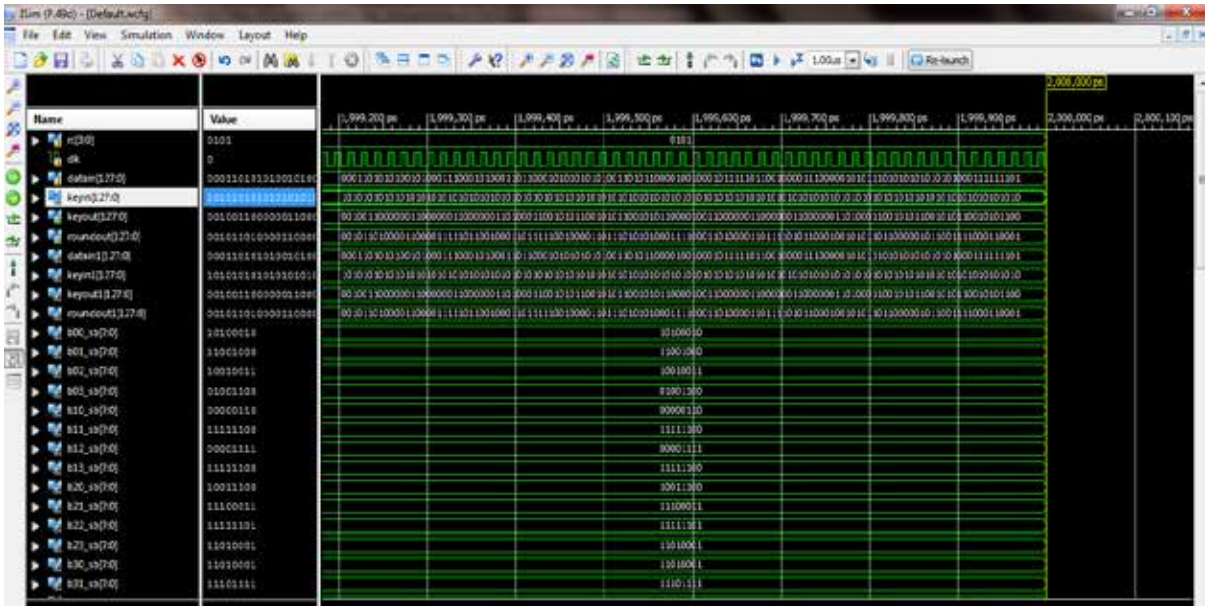
Snapshot is nothing but every moment of the application while running. It gives the clear elaborated of application. It will be useful for the new user to understand for the future steps.

3.1 VARIOUS SNAPSHOTS

Encryption top module

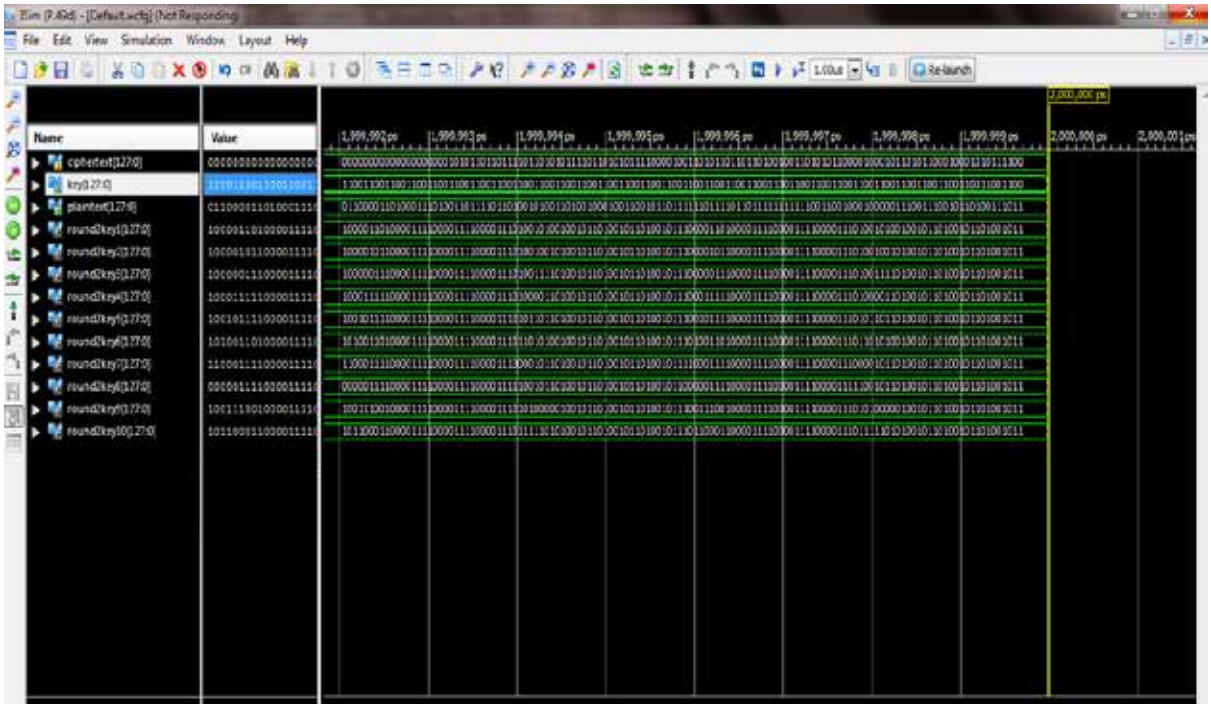


Round operation



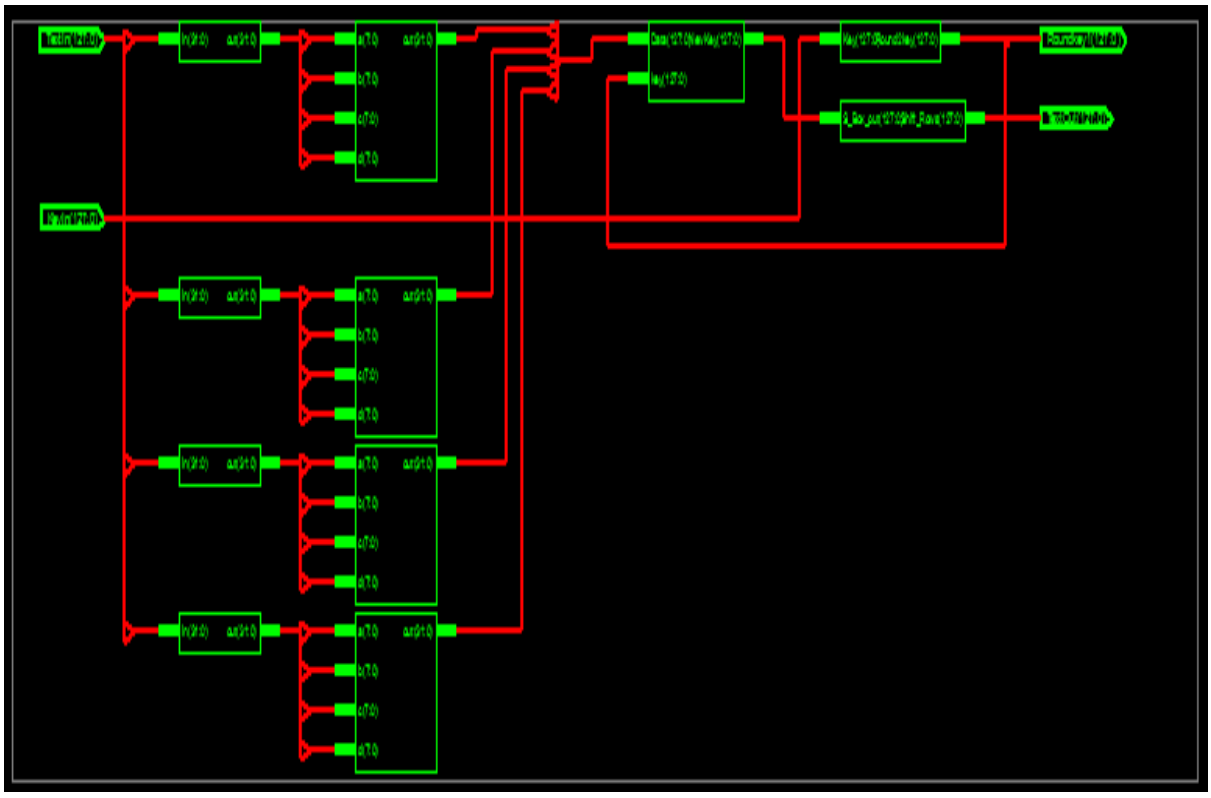
Decryption

Block

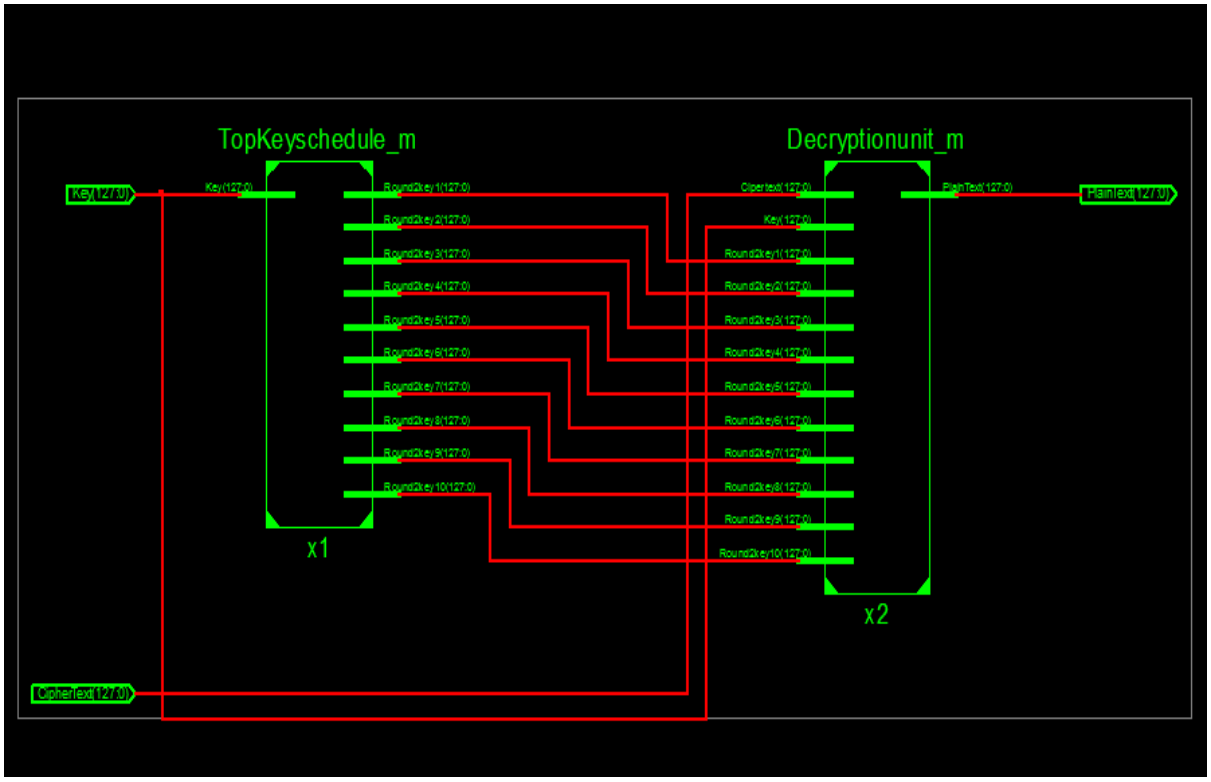


RTL schematic

Encryption:



Decryption:



IV CONCLUSION

The combination of a simple, portable and efficient AES cryptographic algorithm implemented in VHDL source code provides an excellent platform for high security applications. A synthesizable VHDL code is developed for the implementation of both encryption and decryption process. Each program is tested with Spartan 3 FPGA device and output results are verified. Encryption and decryption routines are fully functional at 50 and 100 MHz The software generated key expansion was simulated and run on hardware without the keyboard input and LCD output. Thus, AES can indeed be implemented with reasonable efficiency on an FPGA.

REFERENCES

[1] National Inst. Of Standards and Technology, “Federal Information Processing Standard Publication 197, the Advanced Encryption Standard (AES),” Nov. 2001

[2] J. Daemen and V. Rijmen,” AES Proposal: Rijndael,” AES Algorithm Submission, Sept. 1999

[3] William Stallings, Cryptography and Network Security, Principles and Practices, 4th ed. Pearson Education, pp. 134-161, 2006

[4] Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security, Private Communication in a Public World, 2nd ed. Pearson Education, pp. 41-114, 2006

[5] Wayne Wolf, “FPGA-Based System Design, Pearson Education, pp. 17-37

[6] Xinmiao Zhang and Keshab K. Parhi, “Implementation Approaches for the Advanced Encryption Standard Algorithm,” IEEECircuits and systems Magazine, vol. 2, no. 4, pp. 24–46, 2003

[7] G. Rouvroy, F.-X. Standaert, F.-X.J.– J. Quisquater, J.-D. Legat, "Compact and Efficient Encryption/Decryption Module for FPGA Implementation of the AES Rijndael Very Well Suited for Small Embedded Applications," Proc. ITCC-04 Conf., pp. 583-587, 2004

[8] Chih-Chung Lu and Shau-Yin Tseng, "Integrated Design of AES (Advanced Encryption Standard) Encrypter and Decrypter," Proc. IEEE Int. Conf. on Application-Specific Systems, Architectures, and Processors, (ASAP'02), pp. 277-285, 2002